Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Нормативно-правове забезпечення інформаційної безпеки в Україні

Навчальний посібник

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за освітньою програмою «Безпека державних інформаційних ресурсів»
спеціальності F5 (125) Кібербезпека та захист інформації

Укладачі: С.О. Іванченко, С.Д. Нестеренко, Ю.Ф. Щиголь

Електронне мережеве навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2025

УДК 004.77

Укладачі: *Іванченко Сергій Олександрович*, д-р техн. наук, проф.
Нестеренко Сергій Дмитрович
Щиголь Юрій Федорович, к.ю.н.

Рецензенти *Гавриленко Олексій Вадимович,* к.т.н., заступник начальника управління Департаменту захисту інформації Адміністрації Держспецзв'язку
Зінченко Ярослав Вікторович, к.т.н., с.н.с., начальник Науково-дослідного центру Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ»

Відповідальний редактор *Голь В.Д.*, к.т.н., професор

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 9 від 26.06.2025 *р.)*
за поданням вченої ради ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 10 від 24.04.2025 р.)

Нормативно-правове забезпечення інформаційної безпеки в Україні [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Безпека державних інформаційних ресурсів» спец. F5 (125) Кібербезпека та захист інформації / КПІ ім. Ігоря Сікорського ; уклад.: С.О. Іванченко, С.Д. Нестеренко, Ю.Ф. Щиголь. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2025. – 335 с.

У навчальному посібнику викладено концептуальні засади інформаційної безпеки держави, визначені головні напрямки нормативно-правової діяльності в цій сфері, розглянуто структуру та повноваження органів, що забезпечують інформаційну безпеку в Україні, зроблено акцент на нормативно-правовому обґрунтуванні завдань, які покладено на установи та підрозділи Державної служби спеціального зв'язку та захисту інформації України у цій сфері, а саме: забезпеченні кібербезпеки держави, захисті інформації в інформаційно-комунікаційних системах, криптографічному захисті інформації. У навчальному посібнику надано методичні рекомендації щодо системного вивчення відповідного нормативно-правового забезпечення здобувачами, а також наведені контрольні питання для перевірки рівня засвоєння матеріалу ними. Посібник призначений для здобувачів освітнього рівня бакалавра за спеціальністю 125 Кібербезпека та захист інформації, а також викладачів, які задіяні у викладанні відповідного освітнього компонента.

УДК 004.77

Реєстр. № НП 24/25-611. Обсяг 16 авт. арк.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

© КПІ ім. Ігоря Сікорського, 2025

З М І С Т

стор.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ…….. 10

ВСТУП……..…… 13

РОЗДІЛ 1 ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ ……...…….. 16

1.1 Концептуальні засади забезпечення інформаційної безпеки України. Поняття інформаційної безпеки держави……...……. 16

1.1.1 Основні поняття та терміни у сфері інформаційної безпеки ……... 16

1.1.2 Положення законів та концептуальних нормативно-правових актів України щодо місця інформаційної безпеки у забезпеченні національної безпеки держави. Головні завдання забезпечення інформаційної безпеки в державі... 18

1.2 Система нормативно-правових актів України у сфері інформаційної безпеки ……. 35

1.2.1 Система нормативно-правового забезпечення інформаційної безпеки, загальні положення ….. 35

1.2.2 Класифікація нормативно-правових актів за ієрархією в сфері забезпечення інформаційної безпеки……..... 36

1.2.3 Класифікація нормативно-правових актів та нормативних документів за сферою застосування 43

1.2.4 Класифікація нормативно-правових актів та нормативних документів за призначенням та змістом ……... 46

1.3 Методичні рекомендації щодо вивчення положень основних нормативно-правових актів України в сфері інформаційної безпеки концептуального та конститутивного рівнів ……. 49

1.4 Положення основних нормативно правових актів щодо забезпечення кібербезпеки України 59

1.4.1 Закон України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 року

№ 2163-VIII …….. 59
1.4.2 “Стратегія кібербезпеки України” (указ Президента України від 26 серпня 2021 року № 447/2021) 65
1.4.3 Закон України “Про критичну інфраструктуру” від 18 жовтня 2022 року № 2684-IX (зі змінами й доповненнями) …… 89
1.4.4 “Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури” (постанова КМУ від 19 червня 2019 року № 518) ……. 101
1.5 Інтеграційні процеси нормативно-правових актів України з міжнародними стандартами та вимогами в галузі інформаційної безпеки……. 108
1.5.1 Міжнародні стандарти та вимоги в галузі інформаційної безпеки. Стандарти ЄС …… 108
1.5.2 Методичні рекомендації щодо вивчення базових міжнародних стандартів в сфері інформаційної безпеки ……..…… 109
1.6 Класифікація та повноваження суб’єктів забезпечення інформаційної безпеки України ……..…… 114
1.6.1 Загальна класифікація суб’єктів забезпечення інформаційної безпеки України …… 115
1.6.2 Повноваження суб’єктів державного рівня ……..... 117
1.6.3 Повноваження та завдання Державної служби спеціального зв’язку та захисту інформації України щодо забезпечення ІБ держави ……..… 126
1.6.4 Повноваження юридичних осіб та громадян України …….. 148
1.7 Відповідальність осіб за порушення встановлених законодавством України вимог в сфері інформаційної безпеки……. 157
Висновки до розділу 1…… 162
Запитання для самоперевірки (проведення поточного контролю)……..……. 164

РОЗДІЛ 2 ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ……...…… 167

2.1 Положення основних нормативно правових актів України щодо забезпечення захисту інформації в інформаційних та інформаційно-комунікаційних системах ……..…. 167

2.1.1 ДСТУ 2226-93 “Автоматизовані системи. Терміни та визначення” ……..… 168

2.1.2 “Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” (постанова КМУ від 29 березня 2006 року № 373, зі змінами) ……..... 170

2.1.3 “Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці” (НД ТЗІ 3.6-004-21) …… 177

2.1.4 Категорії об'єктів та інформаційних і інформаційно-комунікаційних систем (далі – ІС) ……..…….. 196

2.1.5 Встановлені класи та можливі стандартні функціональні профілі захищеності інформації в ІКС (НД ТЗІ 2.5-005-99) …… 197

2.2 Методичні рекомендації щодо вивчення положень основних нормативних документів щодо захищеності від несанкціонованого доступу інформації, яка не є державною таємницею, в ІКС ……. 200

2.2.1 НД ТЗІ 2.5-008-2002 “Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2” …….. 202

2.2.2 Порядок класифікації ІС і визначення для них стандартних функціональних профілей захищеності

оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5-005-99) ……..… 204
2.2.3 Встановлені критерії оцінки захищеності інформації в ІС від несанкціонованого доступу (НД ТЗІ 2.5-004-99) ……..…… 205
2.3 Положення нормативно-правового забезпечення щодо створення в ІС комплексних систем захисту інформації, яка є державною таємницею…… 206
2.3.1 Нормативно-правове обґрунтування обов'язковості створення комплексної системи захисту інформації (далі – КСЗІ) в ІКС ……..… 206
2.3.2 Технічні канали витоку інформації. Обґрунтування необхідності впровадження заходів технічного захисту інформації …….. 209
2.3.3 Загальний порядок проведення робіт із технічного захисту інформації в ІС (ДСТУ 3396.0-96, ДСТУ 3396.1-96) ……..... 214
2.4 Положення нормативно-правового забезпечення, щодо організації технічного захисту інформації в Україні…….. 217
2.4.1 Положення "Концепції технічного захисту інформації в Україні" (постанова Кабінету Міністрів України від 8 жовтня 1997 року № 1126).. 218
2.4.2 "Положення про технічний захист інформації в Україні" (указ Президента України від 27 вересня 1999 року № 1229/99) ……..…… 200
2.4.3 Обґрунтування необхідності створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності установ……..…. 223
2.5 Положення нормативно-правового забезпечення щодо створення та супроводження функціонування КСЗІ в ІС... 224
2.5.1 Вимоги нормативно-правових актів щодо створення підрозділів (служб) технічного захисту інформації... 224
2.5.2 Призначення та завдання служби захисту інформації установи ……..…….. 227
2.5.3 Етапи створення КСЗІ в ІКС та їхній нормативно-правовий супровід ……..……. 235

2.6 Методичні рекомендації щодо вивчення головних положень нормативно-правового забезпечення стосовно системи безпеки інформації в ІКС, її моніторингу, аудиту та контролю виконання встановлених вимог……..... 240
2.6.1 Порядок розробки та реалізації положень Політики безпеки інформації в ІКС …….. 240
2.6.2 Порядок розробки та виконання Плану захисту інформації в ІКС ……..…… 241
2.6.3 Порядок організації та здійснення аудиту та моніторингу системи безпеки інформації в ІКС ..… 242
2.6.4 Організація та здійснення контролю виконання встановлених вимог безпеки інформації в ІКС ….. 245
2.7 Державна експертиза у сфері технічного захисту інформації ……..….. 248
2.7.1 Методичні рекомендації щодо вивчення головних положень нормативно-правового забезпечення стосовно організації та порядку проведення робіт з державної експертизи у сфері ТЗІ …… 248
2.7.2 Встановлений нормативними документами порядок проведення експертних робіт у сфері ТЗІ …… 251
Висновки до розділу 2 …… ……... 255
Запитання для самоперевірки (проведення поточного контролю) …… 258

РОЗДІЛ 3 ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ……..... 262
3.1 Загальні положення нормативно-правового забезпечення криптографічного захисту інформації в Україні ……..…….…..... 262
3.1.1 “Положення про порядок здійснення криптографічного захисту інформації в Україні” (указ Президента України від 22 травня 1998 року № 505/98). Категорії інформації, що потребують криптографічного захисту в разі її передачі технічними засобами …….. 262

3.1.2 “Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації” (наказ Адміністрації Держспецзв’язку від 20 липня 2007 року за № 141) …… 264
3.1.3 “Про деякі питання ліцензування господарської діяльності в галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України” (постанова КМУ від 16 листопада 2016 року № 821) …….. 272
3.1.4 Ліцензійні умови господарської діяльності в галузі криптографічного захисту інформації ….. 277
3.2 Нормативно-правове забезпечення здійснення електронного документообігу в державі …….....….. 283
3.2.1 Закон України “Про електронні документи та електронний документообіг” від 22 травня 2003 року № 851-IV ……. 284
3.2.2 ДСТУ 4163:2020 “Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів”. Чинні інструкції щодо документоведення в державних установах.. 287
3.2.3 “Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198) …….. 295
3.2.4 “Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (постанова КМУ від 17 січня 2018 року № 55) …. 301
3.3 Методичні рекомендації щодо вивчення положень основних законодавчих та нормативно-правових

документів стосовно забезпечення використання електронних довірчих послуг у державі ……..…… 305
3.3.1 Методичні рекомендації щодо вивчення положень Закону України “Про електронну ідентифікацію та електронні довірчі послуги” від 05 жовтня 2017 року № 2155-VIII, (зі змінами) ……... 306
3.3.2 Методичні рекомендації щодо вивчення положень “Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності” (постанова КМУ від 01 серпня 2023 року № 798) …….. 308

3.4 Методичні рекомендації щодо вивчення положень основних законодавчих та нормативно-правових документів щодо забезпечення державної експертизи у сфері криптографічного захисту інформації ……... 310
3.4.1 Методичні рекомендації щодо вивчення вимог “Положення про державну експертизу у сфері криптографічного захисту інформації”(наказ Адміністрації Держспецзв’язку від 23 червня 2008 року № 100, зареєстрований в Міністерстві юстиції України 16 липня 2008 року за № 651/15342) ……..... 310
3.4.2 Порядок проведення державної експертизи. Експертний висновок …….. 312
3.4.3 Документи, що розробляються під час проведення експертизи вітчизняних та іноземних засобів КЗІ…….. 318
Висновки до розділу 3 ……. 320
Запитання для самоперевірки (проведення поточного контролю) ……... 323
ВИСНОВОК…….. 326
СПИСОК ВИКОРИСТАНИХ ТА РЕКОМЕНДОВАНИХ ДЖЕРЕЛ……. 328

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система

ВР – Верховна Рада

ВЧ – висока частота

ГУР МО – Головне управління розвідки Міністерства оборони

ГШ ЗСУ – Генеральний штаб Збройних Сил України

ДКР – дослідно-конструкторські роботи

ДСК – для службового користування

ДССЗЗІ – Державна служба спеціального зв’язку та захисту інформації України

ДСУЗ – державна система урядового зв'язку

ДСТУ – Державний Стандарт України

ДТ – державна таємниця

ДТЗС – додаткові технічні засоби та системи

ЗВДТ – Звід відомостей, що становлять державну таємницю

ЗІБ – забезпечення інформаційної безпеки

ЗКЗІ – засіб криптографічного захисту інформації

ЗМІ – засоби масової інформації

ЗСУ – Збройні Сили України

ЗТЗІ – засіб технічного захисту інформації

ЄС – Європейський Союз

ІБ – інформаційна безпека

ІзОД – інформація з обмеженим доступом

ІСЗЗІ – Інститут спеціального зв'язку та захисту інформації імені Ігоря Сікорського

КБУ – кібербезпека України

КЗЗ – комплекс засобів захисту

КЗІ – криптографічний захист інформації

ІКС – інформаційно-комунікаційна система

КМУ – Кабінет Міністрів України

ІС – інформаційна система

КСЗІ – комплексна система захисту інформації

КТЗІ – комплекс технічного захисту інформації

ЛОМ – локальна обчислювальна мережа

МВС – Міністерство внутрішніх справ України

МЗС – Міністерство зовнішніх справ України

Мінцифри – Міністерство цифрової трансформації України

МІП – Міністерство інформаційної політики України

МОН – Міністерство освіти і науки України

НАТО – Організація Північноатлантичного договору

НБ – національна безпека

НБУ – Національний банк України

НД – нормативний документ

НД ПДТР – нормативний документ у сфері протидії технічним розвідкам

НДР – науково-дослідні роботи

НД ТЗІ – нормативний документ у сфері технічного захисту інформації

НКЦКБУ – Національний координаційний центр кібербезпеки України

НСД – несанкціонований доступ

НСКЗ – Національна система конфіденційного зв'язку

НПА – нормативно-правовий акт

НТУУ – Національний технічний університет України

ОБСЄ – Організація з безпеки і співробітництва в Європі

ОВ – особливої важливості

ОІД – об'єкт інформаційної діяльності

ОКІ – об'єкт критичної інфраструктури

ОКІІ – об'єкт критичної інформаційної інфраструктури

ООН – Організація Об'єднаних Націй

ОС – обчислювальна система

ОТЗ – основні технічні засоби

ОТР – організаційно-технічне рішення

ОЕОТ – об’єкт електронно-обчислювальної техніки

ПД – персональні дані

ПДТР – протидія технічним розвідкам

ПЕМВН – побічні електромагнітні випромінювання і наведення

ПЕОМ – персональна електронно-обчислювальна машина

РНБО – Рада національної безпеки і оборони

РСО – режимно-секретний орган

РФ – Російська Федерація

СБІ – системи безпеки інформації

СБУ – Служба безпеки України

CERT-UA – (англ. Computer Emergency Response Team of Ukraine) Команда реагування на комп'ютерні надзвичайні події України

СЗІ – Служба захисту інформації

СЗР – Служба зовнішньої розвідки України

СУІБ – система управління інформаційною безпекою

Т – таємно

ТЗ – технічне завдання

ТЗІ – технічний захист інформації

ТКВІ – технічний канал витоку інформації

ЦТ – цілком таємно

ЕОМ – електронно-обчислювальна машина

ВСТУП

Повномасштабна військова агресія проти незалежної та суверенної України, що була розв'язана Російською Федерацією 24 лютого 2022 року, стала першочерговою загрозою національній безпеці нашої держави. Підступний гібридний характер розв'язаної війни несе загрози всім складовим національної безпеки України: у зовнішньополітичній, державній, воєнній, економічній, продовольчій, екологічній, соціальній та інших сферах діяльності. Особливо гостро в сучасних умовах постають питання забезпечення високого рівня інформаційної безпеки держави.

Виклики та загрози з боку агресора в інформаційній сфері обґрунтовують потребу постійного пошуку та впровадження ефективних контрзаходів, залучення для цієї кропіткою та відповідальної роботи відповідних фахівців, задіяних в усіх секторах інформаційної безпеки держави. Відповідно до положень певних законодавчих та нормативно-правових актів держави чималий обсяг завдань у сфері інформаційної безпеки покладено на фахівців відповідних установ та підрозділів Державної служби спеціального зв'язку та захисту інформації України. Широкий спектр та багатогранність цих завдань потребують пошуку шляхів підвищення ефективності та якості підготовки таких фахівців [1-5, 10, 27, 43-45, 52, 53, 63].

Побудова та зміст цього навчального посібника, як і освітнього компонента "Нормативно-правове забезпечення інформаційної безпеки", для забезпечення викладання якого він призначений, за задумом укладачів, мають на меті:

надати здобувачам вищої освіти, які навчаються в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" за спеціальністю *F5 (125) Кібербезпека та захист інформації*, системних знань концептуальних засад інформаційної безпеки, а також положень законодавчих та нормативно правових актів, що регламентують діяльність установ у різних секторах інформаційної безпеки держави;

надати методичну допомогу здобувачам вищої освіти у формуванні відповідних компетентностей, що дозволять їм після завершення навчання успішно виконувати функціональні обов'язки в межах займаних посад, на які будуть призначені;

надати методичну допомогу викладачам, задіяним у викладанні освітнього компонента "Нормативно-правове забезпечення інформаційної безпеки", для якісної підготовки до навчальних занять та їх проведення на високому методичному рівні.

Завданнями освітнього компонента та навчального посібника є формування та закріплення у здобувачів вищої освіти таких важливих фахових компетентностей [1-5], як:

здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики й стандарти з метою здійснення професійної діяльності в галузі інформаційної або кібербезпеки;

здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної або кібербезпеки;

здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною або кібербезпекою;

здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно зі встановленою політикою інформаційної або кібербезпеки.

Предметом освітнього компонента є організація та застосування системи нормативно-правового регулювання процесів забезпечення інформаційної безпеки держави.

Здобувачі після засвоєння навчального матеріалу освітнього компонента мають сформувати наступні програмні результати навчання:

організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних, у галузі інформаційної або кібербезпеки;

застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки або кібербезпеки для розслідування інцидентів;

використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

аналізувати, аргументувати, приймати рішення під час розв’язання складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Освітній компонент є базовим та необхідним для подальшої реалізації інших професійно-орієнтованих освітніх компонентів, передбачених освітньою програмою підготовки бакалаврів “Безпека державних інформаційних ресурсів” за спеціальністю *F5 (125) Кібербезпека та захист інформації*, таких як: “Технічний захист інформації”, “Безпека спеціального зв'язку”, “Військове стажування” та інших.

У навчально-методичному посібнику розглянуто концептуальні засади інформаційної безпеки держави, зокрема наведено основні терміни й визначення у сфері інформаційної безпеки, з’ясовано сутність та класифікації національних інтересів та загроз інформаційній безпеці, визначені головні напрямки нормативно-правової діяльності в цій сфері.

У рамках вивчення системи забезпечення інформаційної безпеки України проаналізовано вітчизняну нормативно-правову базу в зазначеній сфері, напрями державної політики інформаційної безпеки, розглянуто структуру та повноваження органів, що забезпечують інформаційну безпеку в Україні, зроблено акцент на нормативно-правове обґрунтування завдань у сфері інформаційної безпеки, які покладено на установи та підрозділи Державної служби спеціального зв’язку та захисту інформації України.

У навчальному посібнику системно розглянуто основи нормативно-правового забезпечення таких найважливіших складових національної та інформаційної безпеки держави, як: кібербезпека, захист інформації в інформаційних та інформаційно-комунікаційних системах, криптографічний захист інформації в Україні.

У посібнику використані окремі положення концептуальних законодавчих, нормативно-правових актів, а також головних нормативних документів у цих секторах інформаційної безпеки.

Розділ 1
ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1 Концептуальні засади забезпечення інформаційної безпеки України. Поняття інформаційної безпеки держави

1.1.1 Основні поняття та терміни у сфері інформаційної безпеки

Розуміння змісту основних понять та термінів у сфері інформаційної безпеки держави випливають із положень концептуальних нормативно-правових актів держави, а саме: Конституції України (Основного закону), Закону України "Про інформацію", "Концепції національної безпеки України", "Доктрини інформаційної безпеки України", "Стратегії інформаційної безпеки" та інші. [6 – 18]

Базовим поняттям в сфері інформаційної безпеки є розуміння терміну ***"інформація"***.

Інформація *(відповідно до Закону України "Про інформацію")* ***– це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.***

Більш розширено під ***інформацією розуміють відомості про особу, предмети, технології, ресурси, засоби, події, явища, які відбуваються в усіх сферах діяльності держави, житті суспільства, а також у довкіллі, незалежно від форми надання таких відомостей***. Відомості можуть бути подані у вигляді сигналів, знаків, звуків, зображень та в інший спосіб.

Розуміння суті базового поняття "інформація" надає можливість розуміння суті й інших головних визначень та понять у сфері інформаційної безпеки:

"Інформаційна діяльність" – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави.

Основними напрямами інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний. Держава гарантує свободу інформаційної діяльності в кожному із цих напрямів усім громадянам та юридичним особам у межах їхніх прав, свобод, функцій та повноважень.

"Інформаційний суверенітет" – це невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні,

розвитку та здійсненні національної інформаційної політики відповідно до Конституції України, чинного законодавства України, міжнародного права в національному інформаційному просторі України.

Інформаційний суверенітет України забезпечується проведенням цілісної державної програми відповідно до Конституції України, положень чинного законодавства України, норм міжнародного права шляхом реалізації відповідних доктрин, концепцій, програм, що стосуються національної інформаційної політики. Головною передумовою існування інформаційного суверенітету ***є належний стан інформаційної безпеки держави, суспільства та його громадян***.

"Інформаційна безпека" – це стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається заподіяння шкоди через: неповноту, несвоєчасність та невірогідність інформації, що використовується; негативний інформаційний вплив, негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання, порушення цілісності, конфіденційності та доступності інформації *(визначення наведено із положень Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки").*

"Інформаційна безпека України" – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства й держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії заподіяння шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом *(визначення наведено із положень "Стратегії інформаційної безпеки" (введена в дію указом Президента України від 28 грудня 2021року № 685/2021)).*

В сучасних виданнях можна зустріти більш скорочені визначення терміна *"інформаційна безпека", в тому числі з його приналежністю до особи, суспільства та держави:*

"Інформаційна безпека" – стан захищеності особи, суспільства й держави, за якого досягається інформаційний розвиток (технічний,

інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформативні впливи не завдають їм суттєвої шкоди.

"Інформаційна безпека особи" – це стан захищеності психіки та здоров'я людини від деструктивного інформативного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

"Інформаційна безпека суспільства" – це можливість безперешкодної реалізації суспільством й окремими його членами своїх конституційних прав, пов'язаних із вільним одержанням, обробленням, створенням і поширенням інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

"Інформаційна безпека держави" – це стан її захищеності та інформаційного розвитку, за якого акції інформаційного впливу, спеціальні інформаційні операції, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів та комп'ютерна злочинність не завдають суттєвої шкоди національним інтересам.

Розгляд змісту наведених вище термінів та понять потребують з'ясування змісту терміна "інформаційний вплив" ("деструктивний інформаційний вплив"), як важливої загрози інформаційній безпеці.

"Інформаційний вплив" ("деструктивний інформаційний вплив") – це організоване та цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки) в інформаційно-технологічну інфраструктуру об'єкта впливу або фізичний стан людини.

Інформаційний вплив (деструктивний інформаційний вплив) поділяється на інформативно-технічний та інформативно-психологічний.

Розуміння суті основних визначень та термінів у сфері інформаційної безпеки забезпечує успішне засвоєння навчального матеріалу занять даного освітнього компонента.

1.1.2 Положення законів та концептуальних нормативно-правових актів України щодо місця ІБ у забезпеченні національної безпеки держави. Головні завдання забезпечення ІБ в державі

Роль та місце ІБ у забезпеченні національної безпеки держави визначені у відповідних положеннях концептуальних нормативно-правових актів України, а саме: Конституції України (Основному Законі) 1996 року, Законі України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII (зі змінами) та "Стратегії національної

безпеки України", введеної в дію указом Президента України від 26 травня 2015 року. [8, 9, 11]

Саме в цих законодавчих актах держави визначено, що забезпечення інформаційної безпеки держави є ***головною складовою частиною захисту національної безпеки України.***

На підтвердження вище зазначеного доречно навести зміст відповідних положень даних головних законодавчих актів держави:

Конституції України (Основного Закону):

"……

Стаття 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та ***інформаційної безпеки*** *є найважливішими функціями держави, справою всього Українського народу.*

……".

Закону України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII:

"Стаття 3. Принципи державної політики у сферах національної безпеки і оборони.

……

4. Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, ***інформаційної,*** *екологічної* ***безпеки****, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями.*

……".

Положення вище вказаних законодавчих актів України були покладені в основу таких концептуальних нормативно-правових актів держави: ***"Доктрини інформаційної безпеки України",*** *(введена в дію указом Президента України № 47/2017 від 25 лютого 2017 року) та* ***"Стратегії інформаційної безпеки"*** *(введена в дію указом Президента України від 28 грудня 2021 року № 685/2021).*

В цих нормативно-правових актах в умовах сучасності з урахуванням агресії Російської Федерації проти нашої держави визначені головні пріоритети (завдання) у забезпеченні інформаційної безпеки держави.

"Доктрина інформаційної безпеки України" *(введена в дію указом Президента України № 47/2017 від 25 лютого 2017 року) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями й пріоритети державної політики в інформаційній сфері в*

сучасних умовах.

Національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

забезпечення конституційних прав людини на захист приватного життя;

захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства й держави:

захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

забезпечення вільного обігу інформації, крім випадків, передбачених законом;

розвиток та захист національної інформаційної інфраструктури;

збереження і примноження духовних, культурних і моральних цінностей Українського народу;

забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

зміцнення інформаційних зв’язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

розвиток медіакультури суспільства та соціально відповідального медіасередовища;

формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

створення з урахуванням норм міжнародного права системи й механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

безпечне функціонування і розвиток національного інформаційного простору та його інтеграція в європейський і світовий інформаційний

простір;

розвиток системи стратегічних комунікацій України;

ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

формування позитивного іміджу України у світі, донесення оперативної, достовірної та об'єктивної інформації про події в Україні до міжнародної спільноти;

розбудова системи іншомовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та в супутниковому мовленні за межами України.

Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Пріоритети (головні завдання) державної політики в інформаційній сфері:

1) щодо забезпечення інформаційної безпеки:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;

створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;

розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;

побудова дієвої та ефективної системи стратегічних комунікацій;

розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2) щодо забезпечення захисту й розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

забезпечення функціонування Суспільного телебачення і радіомовлення України, в тому числі його належного фінансування;

створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

розвиток правових інструментів захисту прав людини і громадянина

на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

підвищення медіаграмотності суспільства, сприяння підготовці професійних кадрів для медіасфери з високим рівнем компетентності;

удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами:

розвиток механізмів електронного урядування;

сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

проведення реформи урядових комунікацій;

розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до ухвалення рішень органами державної влади та органами місцевого самоврядування;

сприяння формуванню культури суспільної дискусії.

В ***"Стратегії інформаційної безпеки"*** *(введена в дію указом Президента України від 28 грудня 2021 року № 685/2021) визначені стратегічні цілі у сфері ІБ та завдання щодо їх досягнення на сучасному етапі повномасштабної агресії Росії:*

<u>Стратегічна ціль 1.</u> Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання

національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави й суспільства на інформаційні загрози;

ужиття заходів щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України;

розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі;

підготовка та проведення складовими сил оборони інформаційно-психологічних операцій та інших заходів, спрямованих на запобігання, стримування та відсіч збройної агресії Російської Федерації проти України;

посилення відповідальності за поширення недостовірної інформації (дезінформації);

запровадження дієвих механізмів виявлення, фіксації, обмеження доступу та/або видалення з українського сегмента мережі Інтернет інформації, розміщення якої обмежено або заборонено законом;

ефективна взаємодія державних органів, органів місцевого самоврядування та інститутів громадянського суспільства при формуванні та реалізації державної політики в інформаційній сфері;

унеможливлення розповсюдження та демонстрації інформаційних та аудіовізуальних продуктів (продукції), проведення гастрольних заходів, що популяризують або пропагують державу-агресора та її органи влади, представників органів влади держави-агресора та їхні дії, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України, містять заклики до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, екстремізму, сепаратизму, комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі й ненависті, вчинення терористичних актів, посягання на права та свободи людини й громадянина тощо;

протидія інформаційним кампаніям, спрямованим на залучення та/або втягування громадян України, у тому числі дітей, до не передбачених законами України воєнізованих чи збройних формувань.

Стратегічна ціль 2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності.

Культура є ціннісною основою та підґрунтям консолідації українського суспільства, одним із ключових чинників подолання конфлікту цінностей та утвердження української громадянської ідентичності.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

стимулювання розвитку українського кінематографа, теле- і радіо продукції, зокрема у співпраці з європейськими державами, у тому числі створення якісного та сучасного кіно- й медіаконтенту для дітей та молоді;

підтримка вітчизняного книговидання;

створення умов для зміцнення консолідації українського суспільства;

сприяння вільному розвитку, використанню і захисту мов національних меншин, корінних народів України та вивченню мов міжнародного спілкування;

зміцнення інформаційних зав’язків з українською діаспорою, що сприятиме збереженню її етнокультурної ідентичності;

посилення соціогуманітарної складової внутрішньої політики України, розробка та впровадження цілісної системи соціогуманітарних технологій;

залучення ветеранів війни, насамперед з-поміж учасників антитерористичної операції, здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях, до участі в заходах, спрямованих на формування у громадян України на основі суспільно-державних цінностей української громадянської ідентичності, підвищення рівня готовності громадян України до виконання обов'язку із захисту Вітчизни, незалежності та територіальної цілісності України;

підвищення рівня довіри населення до державних інституцій та правоохоронних органів.

Стратегічна ціль 3. Підвищення рівня медіакультури та медіаграмотності суспільства.

Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіасередовище - бути соціально відповідальним і функціонувати стабільно. За таких умов українське суспільство зможе ефективніше протистояти державі-агресору та залишатися стійким перед широким спектром загроз, зокрема в інформаційній сфері.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

підготовка та проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо;

створення сприятливих умов для здійснення діяльності засобів масової інформації;

створення сприятливих умов для підвищення рівня професійної підготовки медіафахівців;

удосконалення законодавства у сфері реклами, зокрема щодо лібералізації норм у цій сфері та посилення відповідальності за трансляцію прихованої реклами;

стимулювання розвитку соціально відповідального бізнесу серед засобів масової інформації.

Стратегічна ціль 4. Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їхньої безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

удосконалення законодавства про доступ до публічної інформації, узгодження положень нормативно-правових актів з нормами міжнародних актів, обов'язкових для виконання Україною;

удосконалення законодавства про захист персональних даних, а також упровадження ефективних механізмів забезпечення його реалізації;

удосконалення законодавства стосовно правового статусу журналістів, провадження ними своєї професійної діяльності, відповідальності за правопорушення, вчинені проти журналістів, членів їхніх сімей та майна, а також за перешкоджання їхній професійній діяльності;

проведення постійного моніторингу дотримання прав і свобод журналістів, а також інших осіб, які поширюють суспільно важливу інформацію, висвітлюють ситуацію та події на тимчасово окупованих територіях України, а також забезпечення збирання, систематизації,

аналізу, оцінювання відповідної інформації з метою фіксації порушень прав осіб на тимчасово окупованих територіях України та оперативного реагування органами державної влади на дії чи бездіяльність держави-агресора;

удосконалення механізму реалізації зобов'язань України відповідно до Європейської конвенції про транскордонне телебачення;

захист інформаційного простору України від незаконного контенту;

забезпечення інформаційної безпеки, захист прав та свобод, зокрема персональних даних військовослужбовців та представників інших складових сил безпеки та оборони України, ветеранів війни, членів їхніх сімей.

Стратегічна ціль 5. Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загально українського інформаційного простору, а також відновлення їхнього права на інформацію, що дає їм змогу підтримувати зв'язок з Україною.

Одним з основних напрямів внутрішньополітичної діяльності держави є захист прав, свобод і законних інтересів своїх громадян на тимчасово окупованих територіях, реалізація ініціатив щодо реінтеграції цих територій, а також захист прав і свобод корінних народів України.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

утвердження в українському та міжнародному інформаційному просторі стратегічних наративів щодо безальтернативності відновлення територіальної цілісності України;

формування розуміння у закордонних аудиторій статусу тимчасово окупованих територій Автономної Республіки Крим та міста Севастополя (невизнання спроби анексії Російською Федерацією Автономної Республіки Крим та міста Севастополя), а також окремих районів Донецької та Луганської областей (спростування та протидія поширюваному Російською Федерацією наративу "громадянської війни");

створення умов для задоволення потреб населення тимчасово окупованих територій в об'єктивній та достовірній інформації шляхом забезпечення стабільного функціонування національного телебачення та радіомовлення на тимчасово окупованих територіях, на територіях, які розташовані на лінії зіткнення, а також на територіях, які межують із тимчасово окупованою територією Автономної Республіки Крим;

збільшення частки та якості українського інформаційного продукту та його поширення на тимчасово окуповані території, на території, які розташовані на лінії зіткнення, а також на території, які межують із тимчасово окупованою територією Автономної Республіки Крим;

розширення зони наземного ефірного мовлення українських телерадіокомпаній із територій, прилеглих до тимчасово окупованих територій, а також через супутник та інші канали постачання сигналу;

інформування громадян України, зокрема тих, які мешкають на тимчасово окупованих територіях, іноземної аудиторії про ситуацію на тимчасово окупованих територіях та дії України стосовно їх реінтеграції;

інформування громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, про шкоду, завдану злочинними діями Російської Федерації, її окупаційної адміністрації на тимчасово окупованій території Автономної Республіки Крим та міста Севастополя, а також контрольованими нею терористичними організаціями на території Донецької та Луганської областей;

спростування дезінформації, у тому числі ідеологем радянської та сучасної російської історіографії, щодо минулого й сучасного України та її територій, що нині є тимчасово окупованими державою-агресором, які поширюються в українських та іноземних засобах масової інформації;

налагодження зворотного зв'язку з громадянами України, які проживають на тимчасово окупованих територіях;

зміцнення почуття спільності між громадянами України, які проживають на тимчасово окупованих територіях, прилеглих до них територіях України, а також громадянами України, які проживають в інших регіонах України;

формування у громадян України, які проживають на тимчасово окупованих територіях, розуміння безальтернативності відновлення територіальної цілісності України та розуміння майбутнього цих територій у складі України, відсутності сприйняття процесу відновлення територіальної цілісності як загрози для себе, розуміння політики України на період тимчасової окупації та потреби використання тих можливостей, що надає Україна своїм громадянам, які проживають на тимчасово окупованих територіях;

забезпечення громадянами України підтримки відновлення територіальної цілісності України, розуміння політики України щодо звільнення тимчасово окупованих територій, необхідності захисту і повноцінної реалізації національно-культурних, соціальних та політичних прав громадян України, які проживають на тимчасово окупованих територіях.

Стратегічна ціль 6. Створення ефективної системи стратегічних комунікацій.

Основною метою створення та розвитку системи стратегічних комунікацій є гарантування ефективної інформаційної взаємодії та діалогу між органами державної влади, органами місцевого самоврядування та

суспільством з питань, що стосуються кризових ситуацій, а також утвердження позитивного іміджу України, інформаційне сприяння просуванню інтересів держави у світі. Ефективна побудова своєї міжнародної інформаційної діяльності дасть змогу Україні здійснювати проактивні інформаційні заходи, інформувати світову спільноту про події в Україні та на її тимчасово окупованих територіях, прогрес у реформах та позитивні внутрішні зміни в державі попри наявну збройну агресію проти України, про ключові рішення органів державної влади щодо стратегічних питань розвитку держави, що сприятиме кращому розумінню міжнародними партнерами внутрішньої і зовнішньої політики держави, забезпечить міжнародну підтримку та покращить імідж України як надійного і передбачуваного партнера.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

визначення системи взаємодії з питань реагування на кризову ситуацію, післякризову комунікацію, запобігання настанню кризи шляхом аналізу передумов кризи та криз, що мали місце в минулому;

налагодження ефективної взаємодії між органами державної влади вищого рівня, центральними органами виконавчої влади та обласними державними адміністраціями з метою вироблення представниками держави єдиної позиції з питань, що виникають під час кризової ситуації та в післякризовий період;

налагодження ефективної взаємодії між представниками держави та громадськістю шляхом забезпечення системного діалогу між державними органами та засобами масової інформації, журналістами, представниками нових медіа з питань, що виникають під час кризової ситуації та в після кризовий період;

забезпечення стабільного функціонування системи іномовлення України шляхом створення та поширення інформаційного продукту каналами супутникового, ефірного наземного аналогового і цифрового мовлення, мовлення в кабельних мережах за межами України, зокрема англійською, російською та іншими мовами;

створення в системі іномовлення України та забезпечення функціонування служби державного радіомовлення на зарубіжні країни;

забезпечення присутності програм вітчизняних телекомпаній у багатоканальних мережах інших держав шляхом сприяння створенню загальнонаціональними телеканалами супутникових іноземних версій (з урахуванням мови країни розповсюдження) для поширення програм за межами України;

забезпечення інформування світової спільноти про події в Україні та донесення офіційної позиції України до представників іноземних держав і засобів масової інформації;

використання знаку (бренду) України “Ukraine Now” з метою популяризації та просування інтересів України у світі;

розробка та поширення позитивних наративів та інформаційних кампаній за кордоном, які сприятимуть підвищенню рівня впізнаваності та кращому розумінню України серед іноземних аудиторій, а також утвердженню іміджу України як демократичної європейської держави, яка рухається до повноправного членства в ЄС та НАТО, є невід'ємною частиною європейського політичного, економічного, культурного, освітнього та інформаційного простору, бере участь у розв'язанні глобальних проблем і ділиться досвідом у сферах, що є актуальними для міжнародної спільноти.

Стратегічна ціль 7. Розвиток інформаційного суспільства та підвищення рівня культури діалогу.

Досягнення зазначеної цілі здійснюватиметься шляхом виконання таких завдань:

публічне обговорення актуальних проблем суспільного розвитку;

розбудова державним оператором національної цифрової мережі телевізійного мовлення, розвиток і модернізація мережі середньохвильового радіомовлення Національної суспільної телерадіокомпанії України;

забезпечення належного фінансування суспільного мовника;

забезпечення стабільного функціонування національного телебачення та радіомовлення на території України, насамперед її прикордонних регіонів, і поширення на них українського інформаційного контенту;

сприяння створенню системи мовлення територіальних громад, що забезпечуватиме розширення комунікативних можливостей та зниження конфліктності всередині територіальних громад, забезпечення їх інформування;

стимулювання інновацій та забезпечення всебічного розвитку й захисту національної інформаційної інфраструктури, зокрема її телекомунікаційної складової, як сукупності різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних (електронних комунікаційних) мереж, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування;

визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних студій та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та

населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передавання інформації через комп'ютерні мережі, унеможливлення вільного обігу інформаційної продукції, що містить пропаганду війни, національної і релігійної ворожнечі, формування захищеного суспільства від деструктивного впливу дезінформації та маніпулятивної інформації в інформаційному просторі України, а також в умовах запровадження правового режиму воєнного стану;

підтримка академічних та аналітичних досліджень в інформаційній сфері, зокрема з вивчення впливу онлайн-контенту нових засобів масової інформації на суспільство.

Аналіз головних положень вище розглянутих нормативно-правових актів свідчить про те, що ***напрямки роботи щодо забезпечення інформаційної безпеки держави*** є багатовекторними, стосуються діяльності різних суб'єктів інформаційних відносин *(громадян, суспільства, юридичних осіб, державних установ, органів місцевого самоврядування, та інших)* та охоплюють різні сфери функціонування держави: зовнішньополітичну, внутрішньополітичну, економічну, сферу державної безпеки та оборони, соціальну, гуманітарну екологічну тощо.

Зробимо спробу цю багатовекторну, різнопланову модель узагальнити, оптимізувати, зробити більш наочною, зрозумілою, максимально наближеною до повноважень та завдань департаментів, служб та структурних підрозділів Державної служби спеціального зв'язку та захисту інформації України.

З цією метою багатовекторність завдань інформаційної безпеки загалом можна згрупувати у такі напрямки:

1. Створення умов для забезпечення інформаційного суверенітету держави, реалізації державної політики у сфері ІБ та протидії монополізації інформаційної сфери.

2. Створення системи ЗІБ держави, організація та державний моніторинг її функціонування.

3. Організація захисту можливій протиправній діяльності суб'єктів ЗІБ всередині самої системи ЗІБ.

4. Забезпечення конституційних прав громадян на свободу слова, доступу до інформації; недопущення неправомірного втручання

органів державної влади у діяльність ЗМІ та переслідування журналістів.

5. Створення передумов для розвитку національної інформаційної інфраструктури, впровадження новітніх інформаційних технологій.

6. Запобігання, виявлення та припинення протиправної діяльності в сучасному інформаційному просторі, спрямованої на заподіяння шкоди ІБ особи, суспільства та держави *(в тому числі й організація реалізації заходів з кібербезпеки та забезпечення захисту об'єктів критичної інфраструктури).*

7. Організація захисту від технічного проникнення до інформаційних систем органів державного управління з метою реалізації деструктивного інформаційного впливу *(в тому числі організація та забезпечення функціонування системи урядового зв'язку, національної системи конфіденційного зв'язку, впровадження та контроль технологій з криптографічного та технічного захисту інформації).*

8. Забезпечення режиму охорони інформації з обмеженим доступом:

– конфіденційної;

– службової інформації, що є власністю держави;

– інформації, яка є державною таємницею (далі – ДТ)**;**

– надважливої інформації, яка є ДТ *(в тому числі організація та контроль ефективності впровадження заходів ПДТР в усіх установах – суб'єктах системи ПДТР держави)*.

Для реалізації стратегії інформаційної безпеки та виконання вище вказаних завдань інформаційної безпеки держави створена **система забезпечення інформаційної безпеки (*далі – система ЗІБ).*** Система ЗІБ держави створена і розвивається відповідно до положень Конституції України та інших НПА, що регулюють суспільні відносини в інформаційній сфері.

До системи ЗІБ держави належать:

– об'єкти забезпечення ІБ держави;

– суб'єкти забезпечення ІБ держави;

– система нормативно-правового забезпечення її функціонування *(саме про яку йде мова в даному навчальному посібнику).*

До ***об'єктів забезпечення ІБ держави*** належать:

свідомість особи, групи осіб, суспільства в цілому;

інформація (*особиста; відкрита, яка є власністю держави; конфіденційна; з обмеженим доступом: службова та інформація, що містить державну таємницю*);

матеріально-технічна база забезпечення ІБ держави *(інформаційно-комунікаційна інфраструктура держави: персонал та засоби створення, поширення інформації та передачі даних).*

До ***переліку суб'єктів*** відповідно до положень Закону України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII належать:

Президент України;

Верховна Рада України;

Кабінет Міністрів України;

Рада національної безпеки і оборони України;

Міністерства, відомства, центральні органи виконавчої влади (в тому числі Міністерство закордонних справ, Державний комітет телебачення і радіомовлення України; Міністерство інформаційної політики України, Міністерство цифрової трансформації та інші;

суди загальної юрисдикції;

прокуратура України;

місцеві державні адміністрації та органи місцевого самоврядування;

спеціальні служби та міністерства України (СБУ, МВС, СЗР, **ДССЗЗІ;** ЗСУ, інші силові правоохоронні органи).

Є доречним звернути увагу майбутніх фахівців Державної служби спеціального зв'язку та захисту інформації України на завданнях, які прямо або опосередковано пов'язані із роботою фахівців структурних підрозділів ДССЗЗІ, що в тексті підрозділів посібника виділені курсивом та жирним шрифтом. Тобто завдання, які будуть покладені на здобувачів інституту після закінчення навчання та призначення на певні посади.

Тому абсолютно доцільним є ретельне вивчення положень даного навчального посібника, формування системних знань та фахових компетентностей, необхідних для успішного вирішення службових обов'язків. Основу цього складають ґрунтовні знання положень нормативно-правових актів та нормативних документів в сфері ІБ, що і є предметом освітніх компонентів фахового спрямування.

Отже, сфера інформаційної безпеки держави містить чималу кількість відповідних термінів, визначень та понять, розуміння суті яких забезпечує успішне засвоєння навчального матеріалу занять даного

освітнього компонента.

Напрямки роботи щодо забезпечення інформаційної безпеки держави є багатовекторними, вони стосуються діяльності різних суб'єктів інформаційних відносин та охоплюють різні сфери функціонування держави: зовнішньополітичну, внутрішньополітичну, економічну, сферу державної безпеки та оборони, соціальну, гуманітарну екологічну тощо.

Певне місце у цій роботі відведено Державній службі спеціального зв'язку та захисту інформацій. На законодавчому рівні їй надано певні повноваження та визначено важливі завдання у сфері інформаційної безпеки. Ці завдання можна згрупувати у певну кількість напрямків діяльності ДССЗЗІ України, тобто накреслити дорожню карту, за якою й розпочати системне вивчення нормативно-правового забезпечення інформаційної безпеки в державі.

Рух цією дорожньою картою доцільно розпочати із побудови певної зрозумілої *системи нормативно-правових актів України у сфері інформаційної безпеки.* Це зробимо у наступному пункті посібника.

1.2 Система нормативно-правових актів України у сфері інформаційної безпеки

1.2.1 Система нормативно-правового забезпечення ІБ, загальні положення

В Україні функціонує система забезпечення інформаційної безпеки держави, яка розвивається та вдосконалюється відповідно до викликів та загроз національній безпеці на сучасному етапі, а також пріоритетів та завдань, які ставить держава перед собою в інформаційній сфері.

Важливим елементом системи забезпечення ІБ держави є система її нормативно-правового забезпечення. Сучасні джерела наводять різні моделі систем класифікації нормативно-правових актів за певними ознаками та критеріями. Залежно від того, до суб'єктів системи ІБ якого рангу належать їхні автори, наведені моделі мають і відповідні особливості із акцентом на переліки тих НПА, вимоги яких відповідають повноваженням цих суб'єктів та є нормативно-правовим обґрунтуванням їхньої діяльності.

З огляду на те, що підготовка майбутніх фахівців Державної служби спеціального зв'язку та захисту інформації України покликана надати слухачам системні знання та сформувати у них відповідні професійні компетентності, запропонована у цьому навчальному посібнику модель системи нормативно-правового забезпечення ІБ повинна мати відповідні акценти на НПА та нормативні документи, що обґрунтовують завдання,

повноваження та обов'язки структурних підрозділів служби. Саме під таким кутом зору й будемо розглядати систему нормативно-правового забезпечення ІБ держави.

Система нормативно-правового забезпечення ІБ, як і системи нормативно-правового забезпечення в інших сферах функціонування держави, закладають конституційні норми відносин у суспільстві (між його членами й державою, між фізичними та юридичними особами тощо), а також основні принципи відповідних відносин на міждержавному рівні. Тому система нормативно-правового забезпечення ІБ виступає змістовним наповненням будь-яких відносин для держави і є основою, на якій формується законодавство в інших сферах її функціонування.

Для того, щоб система нормативно-правового забезпечення ІБ була зрозумілою та логічною за структурою, зручною для системного накопичення знань та практичного використання, пропонуємо варіант її побудови за такими класифікаційними ознаками нормативно-правових актів та нормативних документів, що діють у сфері національної та інформаційної безпеки держави:

- рівень ієрархії (юридичної сили) НПА;
- сфера (сектор ІБ) застосування НПА та нормативних документів;
- призначення та зміст НПА та нормативних документів.

Докладніше розглянемо побудову системи нормативно-правового забезпечення ІБ за цими класифікаційними ознаками.

1.2.2 Класифікація нормативно-правових актів за ієрархією в сфері забезпечення інформаційної безпеки

В інформаційній сфері головним завданням системи нормативно-правового забезпечення ІБ є обґрунтування законності функціонування усіх складових системи ЗІБ. Ця законність повинна базуватися на сукупності законів і підзаконних нормативних актів, які спрямовані на створення необхідних умов для захисту національних інтересів в інформаційній сфері.

Однією з важливих класифікаційних ознак нормативно-правових актів є ***їх класифікація за юридичною силою***. Юридична сила НПА визначає місце, яке він посідає в ієрархічній (вертикальній) структурі чинного законодавства. Слід зауважити, що в законодавстві України та науковій літературі для характеристики взаємозв'язків НПА різної юридичної сили найчастіше використовується термін «ієрархія».

Відомо, що НПА нижчої юридичної сили не повинен суперечити НПА вищої юридичної сили, не може змінювати або скасовувати його. У

випадку виникнення протиріч між актами неоднакової юридичної сили діє акт, що має вищу юридичну силу.

З огляду на вище сказане, нормативну базу забезпечення інформаційної безпеки України слід розглядати з урахуванням наявної ієрархії нормативних актів. Сукупність ієрархічних рівнів утворюють чітку вертикаль НПА.

Вертикаль надає можливість поступово перейти від концепцій та загальних засадничих положень законодавчих документів найвищого рівня до методичних вказівок та інструкцій в межах конкретної установи на найнижчому.

Відповідно класифікувати НПА в сфері ЗІБ та захисту інформації необхідно згідно з наявною в українському законодавстві ієрархією. Згідно з цією ієрархією можна виділити такі рівні: *концептуальний, конститутивний, інституційний.*

На першому ***концептуальному рівні маємо закони, акти та положення, які визначають та закріплюють концептуальні положення***.

На найвищому рівні знаходяться норми Конституції України та інших найважливіших НПА, в яких закріплені концептуальні положення. Ці документи враховують основні положення міжнародних договорів і угод, які ратифіковані Україною. В їхніх положеннях визначені шляхи забезпечення національної безпеки в усіх сферах, у тому числі й інформаційній. [8]

Основою цього рівня слід вважати ***Конституцію (Основний Закон) України.*** В ній встановлені норми, що стосуються ЗІБ України, та які є визначальними для побудови національної системи ІБ держави. Згідно зі *статтею 17 (розглядалось у попередній лекції)* встановлено, що *ЗІБ є однією з найважливіших функцій держави.*

З точки зору захисту прав людини й громадянина в інформаційній сфері найважливішою є стаття 34 Конституції. В цій статті задекларовано таке твердження: “*Кожному громадянину гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань”*, а також “*Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір”*. Також в цій статті йдеться про обмеження цих прав в інтересах національної безпеки, у тому випадку, коли йдеться про ІзОД або іншу передбачену законом інформацію, власником якої є держава.

До першого рівня можна віднести й розглянуту вище ***Стратегію інформаційної безпеки***. Вона визначає актуальні загрози національній безпеці в інформаційній сфері. Метою стратегії є посилення спроможностей щодо забезпечення ІБ держави. Досягнення мети слід

здійснювати шляхом впровадження заходів щодо стримування та протидії загрозам ІБ України. [10]

Основною метою реалізації завдань Стратегії є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Стратегія інформаційної безпеки визначає стратегічні цілі в цій сфері. Так, одна із стратегічних цілей полягає у необхідність забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації та інших прав та свобод. Досягнення зазначеної цілі слід здійснювати шляхом виконання низки завдань. Серед них можна виділити завдання із забезпечення ІБ, зокрема персональних даних, а також інших категорій інформації щодо захисту прав та свобод громадян.

Стратегія інформаційної безпеки є основою для формування державної політики у сфері ІБ, розроблення проєктів, планів та програм для ЗІБ.

До першого ієрархічного рівня також належать:

“Концепція національної безпеки України” (схвалено постановою Верховної Ради України від 16 січня 1997 року № 3/97-ВР, зі змінами);

Закон України “Про національну безпеку України” від 21 червня 2018 року № 2469-VIII;

“Стратегія національної безпеки України” (введено в дію указом Президента України від 14 вересня 2020 року № 392/2020);

“Доктрина інформаційної безпеки України” (введено в дію указом Президента України від 25 лютого 2016 року № 47/2017);

“Стратегія інформаційної безпеки” (введено в дію указом Президента України від 28 грудня 2021 року № 685/2021).

На другому рівні знаходяться НПА конститутивного характеру. Вони визначають важливі положення щодо забезпечення національної безпеки в інформаційній сфері.

З точки зору розвитку концептуальних засад нормативно-правового регулювання ЗІБ України важливим НПА є Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” від 09 січня 2007 року № 537-V. Цей Закон України є чинним, а його положення в умовах сучасності набувають ще більшої актуальності. В пункті 13 цього Закону визначено, що рішення проблеми ІБ має здійснюватися шляхом:

створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз ІБ, запобігання таким загрозам та

забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

вдосконалення нормативно-правової бази щодо забезпечення ІБ, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

До другого рівня ієрархії також можна віднести:

Закон України "Про інформацію" в редакції від 31 березня 2023 року № 2657-XII. Закладає правові основи інформаційної діяльності. В законі закріплено право на інформацію та на доступ до неї, визначено систему відносин і зобов'язань у цій сфері. Загалом цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. [12]

Закон України "Про захист персональних даних" в редакції від 27 жовтня 2022 року № 2297-VI. Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці, чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів. [16]

Закон України "Про державну таємницю" в редакції від 31 березня 2023 року № 3855-XII. Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. [18]

Закон України *"Про захист інформації в інформаційно-комунікаційних системах"* в редакції від 01 липня 2022 року № 80/94-ВР. Регулює відносини у сферах захисту інформації в ІС. Визначає об'єкти захисту. В якості суб'єктів відносин визначає власників та користувачів інформації та ІС. Також визначає спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому органи. [13]

Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" в редакції від 31 березня 2023 р. № 3475-IV. Визначає статус, основні завдання та принципи діяльності Державної

служби спеціального зв'язку та захисту інформації України (далі ДССЗЗІУ). На неї покладається участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-комунікаційних системах, криптографічного, технічного захисту інформації; створення нормативно-правових та нормативних документів у цій сфері, здійснення державного контролю за станом криптографічного, технічного захисту інформації, а також за дотриманням вимог законодавства у сфері надання послуг електронного цифрового підпису всіма суб'єктами інформаційної діяльності держави. [27]

На третьому рівні ієрархії розташовані НПА та нормативні документи вищих, центральних органів виконавчої влади, організаційно-розпорядчі документи інших державних органів, органів місцевого самоврядування, установ, організацій у сфері ЗІБ.

До третього рівня належать: державні стандарти, окремі укази Президента, постанови Кабінету Міністрів України, накази, розпорядження міністерств та відомств, якими введені в дію певні стандарти, порядки, положення, інструкції, рішення тощо. Вони визначають норми, основні методи, заходи, порядки та шляхи виконання завдань стосовно захисту інформації та забезпечення інформаційної безпеки окремої особи, суспільства, держави.

Органи державної влади, міністерства, відомства України, державні установи в межах визначеної законодавством про ІБ відповідальності та компетенції, а також відповідно то окремих НПА першого та другого рівнів ієрархії, розробляють та впроваджують відомчі накази, інструкції, положення. Вимоги цих відомчих нормативних документів спрямовані на реалізацію захисту життєво важливих інтересів людини, суспільства та держави в інформаційній сфері.

До третього рівня ієрархії можна віднести такі НПА та нормативні документи загальнодержавного використання:

– ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення";

– ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт";

– "Положення про технічний захист інформації в Україні", введено в дію указом Президента України від 27 вересня 1999 року № 1229/99 (зі змінами);

– "Концепція технічного захисту інформації в Україні", введено в дію постановою КМУ від 08 жовтня 1997 року № 1126 (зі змінами);

– "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах",

введено в дію постановою КМУ від 29 березня 2006 року № 373 (зі змінами);

– “Порядок організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, підприємствах, в установах і організаціях”, введено в дію постановою КМУ від 18 грудня 2013 року № 939 (зі змінами);

– чимала низка нормативних документів у сферах ТЗІ (НД ТЗІ), ПДТР (НД ПДТР) та інші нормативні та розпорядчі документи державних органів, міністерств, відомств, департаментів, служб (головні положення основних із них розглядаються у розділах 2 та 3 навчального посібника).

Важливу роль у системі нормативно-правового забезпечення ІБ відіграють акти інституційного рівня місцевих органів влади. Це – рішення місцевих органів влади з питань забезпечення ІБ, які є обов’язковим для виконання всіма установами та організаціями, а також посадовими особами і громадянами на підпорядкованій території.

Кінцевим ланцюгом у переліку нормативних документів третього рівня наведеної ієрархії є організаційно-розпорядчі документи (накази, інструкції, методичні рекомендації тощо) органів державної влади, органів місцевого самоврядування, установ та організацій. Ці організаційно-розпорядчі документи діють в межах повноважень вище вказаних органів, установ та організацій.

На рисунку 1 наведена класифікація НПА держави, чинних у сфері ЗІБ, за ієрархією:



Рис. 1 - Класифікація НПА держави за рівнями ієрархії

Отже, ієрархія НПА у сфері забезпечення інформаційної безпеки визначає фундаментальні підходи до визначення юридичної сили тих чи інших нормативних актів України. Саме юридична сила НПА надає можливість проводити систематизацію цих актів та їх впровадження тими чи іншими установами та організаціями. Державні установи повинні враховувати ієрархію (юридичну силу) НПА, а також чинне законодавство України у сфері ЗІБ та захисту інформацію під час розробки та впровадження власних нормативних та організаційно-розпорядчих документів з цих питань.

1.2.3 Класифікація нормативно-правових актів та нормативних документів за сферою застосування

Другою класифікаційною ознакою запропонованої для розгляду моделі системи нормативно-правового забезпечення ІБ є *сфера застосування (сектор ІБ)* НПА та нормативних документів.

Перелік сфер (секторів ІБ) можна сформувати, виходячи із переліку завдань системи забезпечення ІБ та суб'єктів ІБ, на які покладено відповідальність за організацію впровадження цих завдань у державі.

Для наочності представимо класифікацію за цією ознакою у вигляді Таблиці 1:

Таблиця 1. Класифікація НПА та нормативних документів *за сферою застосування (сектором ІБ)*

Класифікація НПА та нормативних документів за сферою застосування (сектором ІБ)			
№ з/п	**Завдання (сектор) ІБ**	**Категорії НПА та нормативних документів у сфері ІБ**	**Суб'єкти системи ЗБІ, відповідальні за організацію впровадження в державі завдань ІБ, розроблення проєктів законів та НПА**
1	**Створення умов для забезпечення інформаційного суверенітету держави, реалізації державної політики у сфері ІБ та протидії монополізації інформаційної сфери**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, накази та розпорядження голів спецслужб**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування Міністерство закордонних справ; Міністерство інформаційної політики України; Спеціальні служби України (СБУ, МВС, СЗР, ГУР МО, **ДССЗЗІ** та інш.)
2	**Створення системи ЗІБ держави, організація та державний моніторинг її функціонування**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування Міністерство закордонних справ; Міністерство інформаційної політики України; Спеціальні служби України (СБУ, МВС, СЗР, ГУР МО, **ДССЗЗІ**)

3	**Організація захисту можливій протиправній діяльності суб'єктів ЗІБ всередині самої системи ЗІБ**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, НД ТЗІ, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади; органи місцевого самоврядування, установи, організації **ДССЗЗІ**; СБУ, МВС, СЗР, МОУ, ГУР МО
4	**Забезпечення конституційних прав громадян на свободу слова, доступу до інформації; недопущення неправомірного втручання органів державної влади у діяльність ЗМІ та переслідування журналістів**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування Державний комітет телебачення і радіомовлення України; Міністерство інформаційної політики України; Міністерство цифрової трансформації МВС; СБУ; Прокуратура України
5	**Створення передумов для розвитку національної інформаційної інфраструктури, впровадження новітніх інформаційних технологій**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування; Державний комітет телебачення і радіомовлення України; Міністерство інформаційної політики України; Міністерство цифрової трансформації; СБУ, МВС, СЗР, **ДССЗЗІ**, ГУР МО
6	**Запобігання, виявлення та припинення протиправної діяльності в сучасному інформаційному просторі, спрямованої на заподіяння шкоди ІБ особи, суспільства та держави**	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування Державний комітет телебачення і

	(в тому числі організація реалізації заходів з кібербезпеки та забезпечення захисту об'єктів критичної інфраструктури)	**України, постанов КМУ, накази та розпорядження керівників зазначених суб'єктів**	радіомовлення України; Міністерство інформаційної політики України; Міністерство цифрової трансформації; **ДССЗЗІ**; СБУ, МВС, СЗР, ГУР МО
7	**Організація захисту від технічного проникнення до інформаційних систем органів державного управління з метою реалізації деструктивного інформаційного впливу** *(в тому числі організація та забезпечення функціонування системи урядового зв'язку, НСКЗ, впровадження та контроль технологій з криптографічного та технічного захисту інформації)*	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, НД ТЗІ, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади; органи місцевого самоврядування, установи, організації **ДССЗЗІ**; СБУ, МВС, СЗР, МОУ, ГУР МО
8	**Забезпечення режиму охорони інформації з обмеженим доступом:** **-конфіденційної;** **-службової інформації, що є власністю держави;** **-інформації, яка є ДТ;** **-надважливої інформації, яка є ДТ** *(в тому числі організація та контроль ефективності впровадження заходів ПДТР в усіх установах – суб'єктах системи ПДТР держави)*	Укази Закони України Постанови КМУ Накази, розпорядження **Проєкти законів України, постанов КМУ, НД ТЗІ, НД ПДТР, накази та розпорядження керівників зазначених суб'єктів**	Президент України; Верховна Рада України; Кабінет Міністрів України; Міністерства, відомства, центральні органи виконавчої влади; органи місцевого самоврядування, установи, організації **ДССЗЗІ**; СБУ, МВС, СЗР, МОУ, ГУР МО

Наведена класифікація законодавчих, нормативно-правових актів та нормативних документів за ознакою *сфера застосування* наочно дає уявлення про спрямованість їхніх положень на регламентацію діяльності суб'єктів та їхніх взаємовідносин *у певному секторі* інформаційної безпеки держави, а також їхньої участі у формуванні державної політики в цій сфері.

Отже, класифікація чинних законодавчих, нормативно-правових актів та нормативних документів за ознакою сфери застосування (сектор ІБ) надає слухачам (посадовим особам установ) можливості вивчення їхніх положень та системного формування знань, необхідних для виконання завдань у певному секторі ІБ відповідно до покладених на них

посадових обов'язків. А у разі переміщення по службі на інші сектори ІБ, швидко орієнтуватися щодо напрямку та обсягу нарощування своїх професійних знань та адаптації на новій посаді в іншому відділі, управлінні або іншій установі.

Переліки законодавчих, нормативно-правових та нормативних документів, які забезпечують нормативно-правовий супровід завдань (секторів) ІБ налічують від кількох одиниць до декількох десятків найменувань у кожному секторі. Призначення та зміст основних із них будуть розглянуті в подальших розділах навчального посібника.

1.2.4 Класифікація нормативно-правових актів та нормативних документів за призначенням та змістом

Третьою класифікаційною ознакою запропонованої для розгляду моделі системи нормативно-правового забезпечення ІБ є *призначення та зміст* НПА та нормативних документів. Класифікацію документів за цими ознаками доречно використовувати відносно НПА та нормативних документів *конститутивного та інституційного рівнів ієрархії, а також їхньої приналежності до певного сектору (сукупності секторів) ІБ.*

Систематизація НПА та нормативних документів за цією класифікаційною ознакою надає слухачам (фахівцям, задіяним у певних секторах ІБ) можливості використання їх вимог та положень для практичного вирішення конкретних службових завдань різного змісту та направленості, а саме: впровадження конкретних організаційних, інженерно-технічних та інших заходів у певних секторах ІБ, реалізації методик оцінки ефективності впроваджених заходів тощо. Наприклад: організувати роботу комісії щодо проведення спеціальних обстежень певних приміщень в адміністративній будівлі установи; розробити інструкцію користувачу щодо забезпечення безпеки інформації під час роботи на автоматизованому робочому місці ІС установи; провести перевірку забезпечення безпеки інформації під час її обробки в ЛОМ; виконати заходи протидії технічним розвідкам на етапі розгортання та експлуатації рухомої станції зв'язку в польових умовах та інші завдання.

Наведені приклади вже на інтуїтивному рівні в свідомості генерують думки про те, що йдеться про різні за призначенням та змістом нормативні документи. Але фахівці ДССЗЗІ в своїй службовій діяльності не покладаються на інтуїцію та певні припущення, їх професіоналізм будується на твердих знаннях вимог (положень) чинних НПА та нормативних документах у відповідних секторах ІБ. Тому докладно розглянемо суть їхньої класифікації за цією ознакою.

В кожному секторі ІБ всю сукупність нормативних документів загалом відповідно до їхнього *призначення та змісту* можна розподілити за такими основними видами:

1. Основні положення, термінологія.
2. Норми.
3. Методики.
4. Загальні технічні вимоги.
5. Правила, інструкції, порядки, настанови.
6. Методичні вказівки.
7. Рекомендації.

тощо.

До першого виду *(основні положення, термінологія)* належить певна частина стандартів та нормативних документів, що встановлюють термінологію та визначення базових понять у певному секторі ІБ, визначають основні положення щодо організації та забезпечення впровадження відповідних заходів, встановлюють службові категорії посадових осіб установ, відповідальних за організацію впровадження заходів ІБ в установі.

Норми – вид нормативних документів, якими встановлюються граничні допустимі значення *(нормовані значення)* певного показника, який передбачений затвердженою Методикою контролю (оцінки, перевірки тощо).

Методики – частина нормативних документів, призначених для здійснення заходів оцінювання (контролю, перевірки, атестації, тощо), шляхом порівняння отриманих результатів із встановленими вимогами, нормами або нормованими значеннями та подальшим висновком щодо їхньої відповідності (або невідповідності).

Загальні технічні вимоги – вид нормативних документів, у положеннях яких визначені загальні вимоги щодо розгортання, монтажу, поточної експлуатації, технічного обслуговування, ремонту тощо, технічних засобів обробки інформації, допоміжних технічних засобів, систем, ліній зв'язку, мереж електроживлення іншого інженерно-технічного обладнання об’єктів інформаційної діяльності установ.

Правила, інструкції, порядки, настанови – вид нормативних документів, які визначають обов’язкові вимоги щодо покрокового виконання заходів інформаційної безпеки в певному її секторі.

Методичні вказівки – вид нормативних документів, у яких надаються вказівки з метою правильного та точного вирішення певних складних

завдань інформаційної безпеки в певному секторі. Методичні вказівки зазвичай є похідною *правил, інструкцій, порядків, настанов.*

Рекомендації – вид нормативних документів, положеннями яких встановлюються основні положення щодо вибору способів і засобів реалізації заходів у певному секторі ІБ.

Кожний вид нормативних документів займає своє місце в загальній системі нормативно-правового забезпечення ІБ держави, має своє призначення та сферу практичного використання. За назвою та приналежністю нормативного документа до певного виду фахівець може заздалегідь передбачити його обсяг, спрямованість та корисність для пошуку необхідних положень для обґрунтованого оперативного виконання певних службових завдань.

Отже, систему нормативно-правових актів України у сфері інформаційної безпеки доцільно побудувати за класифікаційними ознаками: рівень ієрархії (юридичної сили), сфера (сектор ІБ) застосування, призначення та зміст НПА та нормативних документів.

Класифікація за ієрархією визначає фундаментальні підходи до визначення юридичної сили тих чи інших нормативних актів України. Суб'єкти інформаційних відносин повинні враховувати ієрархію (юридичну силу) НПА, а також чинне законодавство України у сфері ЗІБ та захисту інформації під час розробки та впровадження власних нормативних та організаційно-розпорядчих документів з цих питань.

Класифікація чинних законодавчих, нормативно-правових актів та нормативних документів за ознакою сфера застосування (сектор ІБ) надає можливості для вивчення їхніх положень та системного формування знань, необхідних для виконання завдань у певному секторі ІБ відповідно до покладених на фахівців посадових обов'язків. А в разі переміщення по службі на інші сектори ІБ, швидко орієнтуватися щодо напрямку та обсягу нарощування своїх професійних знань та адаптації на новій посаді в іншому відділі, управлінні або іншій установі.

Класифікація за назвою та приналежністю нормативного документа до певного виду надає можливість фахівцям пришвидшити пошук необхідних положень НПА для обґрунтованого виконання певних службових завдань.

Знання принципів побудови системи нормативно-правових актів України у сфері інформаційної безпеки озброює здобувачів певним інструментом подальшого системного вивчення положень чинних НПА та нормативних документів в цій сфері, сприяє формуванню у них професійних знань, відповідних компетентностей фахівців ДССЗЗІ України.

1.3 Методичні рекомендації щодо вивчення положень основних нормативно-правових актів України в сфері ІБ концептуального та конститутивного рівнів

З'ясувавши класифікацію нормативно-правових актів України в сфері ІБ, є логічним докладно розглянути призначення та основні положення цілої низки нормативно-правових актів України, які є базовими, складають правову основу державної політики у сфері національної та інформаційної безпеки, а також діяльності суб'єктів інформаційних відносин в кожному її секторі. Ця низка складається із НПА концептуального та конститутивного рівнів [8 - 18], а саме:

Конституція України (Основний закон) (ухвалено на п'ятій сесії Верховної Ради України 28 червня 1996 року) (зі змінами);

"Стратегія національної безпеки України" (введено в дію указом Президента України від 14 вересня 2020 року № 392/2020);

"Доктрина інформаційної безпеки України" (введено в дію указом Президента України від 25 лютого 2016 року № 47/2017);

"Стратегія інформаційної безпеки" (введено в дію указом Президента України від 28 грудня 2021 року № 685/2021);

Закон України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII (зі змінами);

Закон України "Про інформацію" від 02 жовтня 1992 року № 2657-XII (зі змінами);

Закон України "Про захист інформації в інформаційно-комунікаційних системах" від 05 липня 1994 року № 80/94-ВР (зі змінами);

Закон України "Про електронні комунікації" від 16 грудня 2020 року № 1089-IX (зі змінами);

Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV (зі змінами);

Закон України "Про захист персональних даних" від 01 червня 2010 року № 2297-VI (зі змінами);

Закон України "Про Національну систему конфіденційного зв'язку" від 10 січня 2002 року № 2919-III (зі змінами);

Закон України "Про державну таємницю" від 21 січня 1994 року № 3856-XII (зі змінами).

Вивчення положень вищевказаних законодавчих та нормативно-правових актів доцільно здійснити в процесі проведення декількох групових практичних занять. В ході цих занять викладач організовує засвоєння курсантами (слухачами) головних положень НПА шляхом виконання ними спеціально сформульованих завдань та сприяє формуванню у курсантів умінь і навичок системного накопичення необхідних професійних знань з метою їх практичного застосування у

подальшій службі. В ході роботи курсантів викладач контролює вивчення курсантами головних положень НПА, задає контрольні питання, оцінює відповіді курсантів, заохочує активність курсантів. У разі запитань з боку курсантів, надає відповіді та пояснення, наводить наочні приклади.

Пропонуємо такий обсяг завдань щодо вивчення призначення та головних положень НПА під час групових практичних занять, а також переліки питань для проведення контролю (самоконтролю) якості вивчення матеріалу.

Обсяг завдань щодо вивчення положень ***Конституції України (Основного Закону) від 28 червня 1996 року № 254к/96-ВР (зі змінами)****:*

– вивчити загальну побудову змісту Конституції, найменування її розділів;

– детально опрацювати:

Розділ І. ЗАГАЛЬНІ ЗАСАДИ (особливу увагу звернути на зміст ст. 17);

Розділ ІІ. ПРАВА, СВОБОДИ ТА ОБОВ'ЯЗКИ ЛЮДИНИ І ГРОМАДЯНИНА (особливу увагу звернути на зміст ст. ст. 21, 31 –36);

Контрольні питання:

– яке місце займає ІБ в переліку напрямків діяльності щодо забезпечення національної безпеки держави (ст. 17)?

– які конституційні права має громадянин України в інформаційній сфері діяльності держави (ст.ст. 31, 32, 34 – 36)?

Обсяг завдань щодо вивчення положень ***Закону України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII:***

– вивчити призначення Закону, загальну побудову його змісту, найменування розділів;

– детально опрацювати:

Розділ ІІ. ЗАСАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ (особливу увагу звернути на зміст ст. ст. 2, 3);

Розділ IV. СЕКТОР БЕЗПЕКИ І ОБОРОНИ (особливу увагу звернути на зміст ст. 22);

Розділ V. ПЛАНУВАННЯ У СФЕРАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ (особливу увагу звернути на зміст ст. ст. 27, 31).

Контрольні питання та завдання:

1. *Доповісти про призначення Закону (вступна частина до Закону).*
2. *Доповісти про основні принципи, що визначають порядок формування державної політики у сферах національної безпеки і оборони держави (ст. 3).*
3. *Які завдання у сфері національної безпеки держави покладені на ДССЗЗІ України (ст. 22)?*

4. *Які заходи передбачає комплексний огляд сектору безпеки та оборони (ст. 27)?*
5. *На які суб'єкти держави покладені повноваження щодо визначення порядку огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (ст. 27, пункт 3)?*
6. *Які концептуальні положення містить Закон щодо призначення та змісту стратегії кібербезпеки в Україні (ст. 31 п.п. 1, 3)?*

Обсяг завдань щодо вивчення положень ***"Стратегії національної безпеки України" (введено в дію указом Президента України від 26 травня 2015 року)***:

– вивчити призначення, загальну побудову змісту Стратегії, найменування її розділів;

– опрацювати:

Розділ І. Пріоритети національних інтересів України та забезпечення національної безпеки, цілі та основні напрями державної політики у сфері національної безпеки (особливу увагу звернути на зміст п. п. 1, 5, 6);

Розділ ІІ. Поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов (особливу увагу звернути на зміст п. п. 17, 19, 20, 27);

Розділ ІІІ. Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки (особливу увагу звернути на зміст п. п. 33, 34, 45 – 48, 51, 52, 57);

Розділ IV. Напрями та завдання реформування й розвитку сектору безпеки і оборони (особливу увагу звернути на зміст п. 63);

Контрольні питання та завдання:

1. *Яка головна мета державної політики національної безпеки (п. 1)?*
2. *Що є пріоритетами національних інтересів України та забезпечення національної безпеки (п. 5)?*
3. *Які чинники є об'єктивними зовнішніми загрозами та складовими гібридної війни країни-агресора проти нашої держави (п. п. 17, 19, 20)?*
4. *Доповісти про напрямки запобігання спробам країни-агресора спровокувати внутрішні конфлікти в Україні (п. 45).*
5. *Доповісти про напрямки забезпечення інформаційно-психологічної безпеки громадян, які визначені Стратегією (п. 46).*
6. *Якою важливою складовою зі сфери інформаційних відносин повинна володіти запроваджена в державі національна система стійкості до реагування на широкий спектр загроз на сучасному етапі (п. 47)?*
7. *Яке завдання розвитку системи кібербезпеки на сучасному етапі в*

Стратегії визначено як основне (п. 52)?

8. *Які напрямки діяльності держави в сфері інформаційних відносин в Стратегії вказані як пріоритетні в сучасних умовах (п. 63)?*

Обсяг завдань щодо вивчення положень ***"Доктрини інформаційної безпеки України" (введено в дію указом Президента України від 25 лютого 2016 року № 47/2017)***:

– вивчити призначення Доктрини;

– зміст Доктрини опрацювати в повному обсязі.

Контрольні питання та завдання:

1. *Доповісти про призначення Доктрини (розділ 1, 4-й абзац).*
2. *Доповісти про мету та принципи, закладені в Доктрину (розділ 2).*
3. *Доповісти про національні інтереси України в інформаційній сфері (розділ 3).*
4. *Доповісти про головні загрози національним інтересам та національній безпеці України в інформаційній сфері (розділ 4).*
5. *Доповісти про головні пріоритетні напрямки державної політики в інформаційній сфері (розділ 5, пункти 1), 2), 3), 4) без деталізації заходів).*
6. *Доповісти про перелік суб'єктів системи інформаційної безпеки держави, на яких покладено певні повноваження щодо впровадження положень Доктрини (розділ 6).*

Обсяг завдань щодо вивчення положень ***"Стратегії інформаційної безпеки" (введено в дію указом Президента України від 28 грудня 2021 № 685/2021)***:

– вивчити призначення Стратегії;

– зміст Стратегії опрацювати в повному обсязі.

Контрольні питання та завдання:

1. *Доповісти про призначення Стратегії (Загальні положення, 1-й абзац).*
2. *Доповісти про мету Стратегію та чим ця мета досягається (Загальні положення, 2-й, 3-й абзаци).*
3. *Доповісти про глобальні виклики та загрози в інформаційній сфері (розділ "Аналіз загроз та викликів інформаційній безпеці. Глобальні виклики та загрози").*
4. *Доповісти про національні виклики та загрози в інформаційній сфері (розділ "Національні виклики та загрози").*
5. *Доповісти про стратегічні цілі та напрями реалізації Стратегії (розділ "Стратегічні цілі та напрями реалізації Стратегії", цілі 1-7 без деталізації заходів).*
6. *Доповісти про перелік суб'єктів системи інформаційної безпеки держави, на яких покладено певні повноваження щодо впровадження*

положень Стратегії (розділ "Механізми реалізації визначеної мети та завдань").

7. *Доповісти про очікувані результати впровадження положень Стратегії (розділ "Очікувані результати").*

Обсяг завдань щодо вивчення положень ***Закону України "Про інформацію" від 02 жовтня 1992 року № 2657-XII (зі змінами):***

– вивчити призначення Закону;

– зміст Закону опрацювати в повному обсязі.

Контрольні питання та завдання:

1. *Доповісти про призначення Закону (1-й абзац тексту Закону).*
2. *Доповісти про основні принципи інформаційних відносин у державі (розділ I, ст.2).*
3. *Доповісти про основні напрями державної інформаційної політики, що визначені Законом (розділ I, ст. 3).*
4. *Доповісти про перелік суб'єктів інформаційних відносин у державі (розділ I, ст.4).*
5. *Чим забезпечуються гарантії прав суб'єктів інформаційних відносин на інформацію (розділ I, ст. 6)?*
6. *Доповісти про основні види інформаційної діяльності (розділ I, ст. 9).*
7. *Доповісти про види інформації за змістом (розділ II, ст. 10).*
8. *Які відомості складають інформацію про фізичну особу (розділ II, ст. 11)?*
9. *Які відомості складають інформацію про товар (роботу, послугу) (розділ II, ст. 14)?*
10. *Які відомості складають критичну технологічну інформацію (розділ II, ст. 19)?*
11. *Доповісти про види інформації за порядком доступу до неї (розділ II, ст. ст. 20, 21 пункти 1-3).*
12. *Які відомості не можуть бути віднесені до інформації з обмеженим доступом (розділ II, ст. 21 пункти 4-6)?*
13. *Надати тлумачення поняттям "Масова інформація", "Засоби масової інформації" (розділ III, ст. ст. 22, 23).*
14. *Яка відповідальність установлена за порушення законодавства про інформацію (розділ IV, ст. 28)?*
15. *За яких обставин суб'єкти звільняються від відповідальності за розголошення інформації (розділ IV, ст. 30)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про захист інформації в інформаційно-комунікаційних системах" від 05 липня 1994 року № 80/94-ВР:***

– вивчити призначення Закону;

– опрацювати Закон в повному обсязі;
– детально опрацювати зміст ст. ст. 2, 3, 8-11);

Контрольні питання та завдання:

1. *Яке місце займає даний Закон у системі НПА, чинних у сфері ІБ держави (відповідь надати із урахуванням навчального матеріалу лекції Т1з2 та першого абзацу положень Закону)?*
2. *Що є об'єктами захисту в ІКС (ст. 2)?*
3. *Хто є суб'єктами відносин у разі використання ІКС (ст. 3)?*
4. *Які питання лежать в основі відносин між власником системи та користувачем у разі використання ІКС (ст. 6)?*
5. *Які умови обробки державних інформаційних ресурсів або інформації з обмеженим доступом в ІКС є обов'язковими (ст. 8, перший та другий абзаци, КСЗІ)?*
6. *Пояснити зміст виразу: "застосування комплексної системи захисту інформації з підтвердженою відповідністю" (ст. 8, від третього абзацу до кінця статті).*
7. *Які найважливіші організаційні заходи повинен вжити власник ІКС для забезпечення захисту інформації в системі (ст. 9, СЗІ) і це є головною вимогою можливості створення та функціонування КСЗІ в ІКС?*
8. *Проаналізувати головні функції та повноваження спеціального уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації в державі (ст. 10), дати його повну назву.*
9. *Як ви класифікуєте випадки, коли суб'єкти інформаційних відносин не виконують встановлені Законом вимоги забезпечення безпеки інформації, що обробляється в ІКС; ваші припущення щодо можливих наслідків для порушників (ст. 11)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про електронні комунікації" від 16 грудня 2020 року № 1089-IX (зі змінами):***

– вивчити призначення та сферу дії Закону (перший абзац тексту закону та ст. 1 Розділу І. ЗАГАЛЬНІ ПОЛОЖЕННЯ);

– ознайомитись із загальною побудовою змісту Закону (з'ясувати кількість та найменування розділів);

– детально опрацювати:

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ (особливу увагу звернути на зміст ст. ст. 2, 4);

Розділ ІІ. ДЕРЖАВНЕ УПРАВЛІННЯ І РЕГУЛЮВАННЯ У СФЕРАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ТА РАДІОЧАСТОТНОГО СПЕКТРА (особливу увагу звернути на зміст ст. ст. 5, 6);

Розділ VIII. ДЕРЖАВНЕ УПРАВЛІННЯ ТА РЕГУЛЮВАННЯ У СФЕРІ РАДІОЧАСТОТНОГО СПЕКТРА (особливу увагу звернути на зміст ст. 43,

п. 4);

Розділ XIV. ПОСЛУГИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ТА КІНЦЕВІ КОРИСТУВАЧІ ПОСЛУГ (особливу увагу звернути на зміст ст. 104 п. 6, ст. 105);

Розділ XV. КОНФІДЕНЦІЙНІСТЬ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ (особливу увагу звернути на зміст ст. ст. 119, 120);

Розділ XVII. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЕЛЕКТРОННІ КОМУНІКАЦІЇ (складається із ст. ст. 126, 127).

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії Закону (перший абзац тексту закону та ст. 1 Розділу I).*
2. *Доповісти про загальну побудову змісту Закону, кількість та найменування розділів (складається із 19 розділів на 164 сторінках, назви розділів).*
3. *Доповісти про повноваження Кабінету Міністрів України з реалізації державного управління і регулювання у сферах електронних комунікацій та радіочастотного спектра (ст. 5).*
4. *Доповісти про перелік суб'єктів інформаційних відносин, які положеннями Закону віднесені до категорії спеціальних користувачів радіочастотного спектра (ст. 43, ДССЗЗІ).*
5. *Доповісти про загальні засади надання електронних комунікаційних послуг кінцевим користувачам (ст. 104).*
6. *Які відомості щодо умов та правил надання (отримання) електронних комунікаційних послуг має право вимагати кінцевий користувач від органів державної влади або органів місцевого самоврядування (ст. 105)?*
7. *Доповісти про перелік даних про кінцевого користувача, яким постачальники електронних комунікаційних послуг повинні забезпечити надійне зберігання та нести за це відповідальність (ст. 119).*
8. *Які заходи щодо захисту кінцевих користувачів від спаму передбачені Законом (ст. 120)?*
9. *Яка відповідальність суб'єктів інформаційних відносин встановлена Законом за порушення законодавства про електронні комунікації (ст. 126)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV***:

– вивчити призначення та сферу дії Закону (перший абзац тексту

закону та ст. 2 Розділу І. ЗАГАЛЬНІ ПОЛОЖЕННЯ);

– ознайомитись із загальною термінологією та побудовою змісту Закону (з'ясувати кількість та найменування розділів);

– опрацювати усі розділи Закону.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії Закону (перший абзац тексту закону та ст. 2 Розділу І).*
2. *Доповісти про загальну побудову змісту Закону, кількість та найменування розділів (складається із 5 розділів на 5 сторінках, назви розділів).*
3. *Які суб'єкти інформаційних відносин здійснюють державне регулювання електронного документообігу (ст. 4)?*
4. *Надайте пояснення, що розуміємо під терміном "електронний документ" (ст. 5).*
5. *Що розуміємо під терміном "електронний підпис документа" (ст. 6)?*
6. *Що розуміємо під терміном "оригінал електронного документа" (ст. 7)?*
7. *Що являє собою електронний документообіг (обіг електронних документів) (ст. 9)?*
8. *Доповісти про передбачені законом процедури відправлення, передавання та отримання електронних документів (ст. ст. 10, 11).*
9. *Які вимоги встановлені законом щодо організації обігу електронних документів, що містять інформацію з обмеженим доступом (ст. 15)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про захист персональних даних" від 01 червня 2010 року № 2297-VI:***

– вивчити призначення та сферу дії Закону (ст. 1);

– ознайомитись із загальною термінологією та побудовою змісту Закону);

– опрацювати усі статті Закону.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії Закону (ст. 1).*
2. *Доповісти про загальну побудову змісту Закону.*
3. *На положеннях яких НПА будуються положення даного закону (ст. 3)?*
4. *За якими категоріями даний Закон класифікує суб'єктів інформаційних відносин, які пов'язані із персональними даними (ст. 4)?*
5. *Що є об'єктами захисту в цій сфері (ст. 5 п. п. 1-3)?*
6. *Які персональні дані не належать до інформації з обмеженим доступом (ст. 5 п. 3 другий та третій абзац)?*
7. *Доповісти про загальні та особливі вимоги до обробки персональних даних (ст. ст. 6, 7).*

8. *Доповісти про права суб'єкта персональних даних (ст. 8).*
9. *Які обставини є підставами для обробки персональних даних (ст. 11)?*
10. *Доповісти про порядок доступу до персональних даних (ст. 16).*
11. *Який порядок забезпечення захисту персональних даних (ст. 24)?*
12. *Яка відповідальність встановлена за порушення законодавства про захист персональних даних (ст. 28)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про Національну систему конфіденційного зв'язку" від 10 січня 2002 року № 2919-III:***

– вивчити призначення та сферу дії Закону (перший абзац тексту закону та ст. 2);

– ознайомитись із загальною термінологією та побудовою змісту Закону);

– опрацювати усі статті Закону.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії Закону (перший абзац тексту Закону та ст. 2).*
2. *Доповісти про загальну побудову змісту Закону (складається із 11 статей на 4 сторінках).*
3. *На вимогах яких НПА будуються положення даного Закону (ст. 3)?*
4. *Доповісти про склад Національної системи конфіденційного зв'язку (ст. 5).*
5. *Доповісти про забезпечення управління Національною системою конфіденційного зв'язку (ст. 6).*
6. *Доповісти про організацію надання послуг конфіденційного зв'язку (ст.7).*
7. *Які види відповідальності за порушення законодавства у сфері конфіденційного зв'язку передбачені Законом (ст. 8)?*

Обсяг завдань щодо вивчення положень ***Закону України "Про державну таємницю" від 21 січня 1994 року № 3856-XII:***

– вивчити призначення та сферу дії Закону (перший абзац тексту закону та ст. 3);

– опрацювати усі статті Закону.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії Закону (перший абзац тексту та ст. 3).*
2. *Дайте визначення терміну "державна таємниця" (ст. 1).*
3. *Дайте пояснення суті термінів "допуск до державної таємниці" та "доступ до державної таємниці" та поясніть, в чому принципова різниця (ст. 1).*

4. *Доповісти про перелік основних суб'єктів інформаційних відносин держави та їхньої компетенції у сфері охорони державної таємниці (ст. 5).*
5. *Які категорії відомостей не можуть бути віднесені до державної таємниці (ст. 8)?*
6. *Поясніть, хто такий "державний експерт з питань таємниць", та які його основні повноваження (ст. 9)?*
7. *Доповісти про загальний порядок віднесення інформації до державної таємниці (ст. 10).*
8. *Доповісти про призначення та порядок формування Зводу відомостей, що становлять державну таємницю (ст. 12).*
9. *Які терміни дії рішення про віднесення інформації до державної таємниці, які дії передбачаються після вичерпання граничного терміну дії рішення (ст. 13)?*
10. *Доповісти про визначений Законом порядок засекречування та розсекречування матеріальних носіїв інформації (ст. 15).*
11. *Доповісти про основні організаційно-правові заходи щодо охорони державної таємниці (ст. 18).*
12. *Доповісти про послідовність дій щодо впровадження дозвільного порядку провадження діяльності, пов'язаної з державною таємницею (ст. 20).*
13. *Які форми допуску громадян до державної таємниці існують, на який граничний термін вони надаються (ст. 22)?*
14. *Які обов'язкові процедури передбачено Законом щодо надання допуску до державної таємниці (ст. 22)?*
15. *За яких умов громадянину може бути надана відмова у наданні допуску до державної таємниці (ст. 23)?*
16. *Доповісти про підстави переоформлення допуску до державної таємниці, підвищення або зниження його форми або скасування (ст. 26)?*
17. *Ким та в якому порядку надається доступ громадянам до державної таємниці (ст. 27)?*
18. *Доповісти про обов'язки громадянина щодо збереження державної таємниці (ст. 28).*
19. *Які суб'єкти інформаційних відносин уповноважені здійснювати контроль за забезпеченням охорони державної таємниці (ст. 37)?*
20. *Які порушення законодавства про державну таємницю передбачають дисциплінарну, адміністративну або кримінальну відповідальність посадових осіб (ст. 39)?*

Знання призначення, встановленої термінології та змісту статей базових законодавчих та нормативно-правових актів України сприяє

успішному вивченню здобувачами положень інших важливих НПА у сфері ІБ держави.

1.4 Положення основних нормативно-правових актів щодо забезпечення кібербезпеки України

З-поміж дев'яти названих у п. 1.1.2 цього посібника завдань (секторів ІБ) особливої уваги потребує шосте завдання: "*Запобігання, виявлення та припинення протиправної діяльності в сучасному інформаційному просторі, спрямованої на заподіяння шкоди ІБ особи, суспільства та держави* ***(в тому числі й організація реалізації заходів з кібербезпеки)****"*. З розпочатою повномасштабною агресією Росії проти нашої держави реалізація цього завдання набула особливої актуальності та важливості.

Докладно розглянемо вимоги законодавчих та нормативно-правових актів держави, які є чинними в цьому секторі ІБ.

1.4.1 Закон України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII

Вивчення положень цього базового законодавчого акту конститутивного рівня доцільно розпочати зі з'ясування поняття ***"****кібербезпека держави"*.

Визначення: ***Кібербезпека держави – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.***

Закон України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017року № 2163-VIII визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі; основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері; основні засади координації їхньої діяльності із забезпечення кібербезпеки. [19]

Вимоги Закону базуються на положеннях Конституції України, низки НПА України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої

встановлена законом, Конвенції про кіберзлочинність, інших міжнародних договорів та згод.

Положення Закону сформульовані в тексті 15 статей, прикінцевих та перехідних положень. Назви статей розкривають формулювання основних термінів, організаційних засад та вимог з питань кібербезпеки у такому порядку:

Стаття 1. Визначення термінів.

Стаття 2. Принципи застосування Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України.

Стаття 4. Об'єкти кібербезпеки та кіберзахисту.

Стаття 5. Суб'єкти забезпечення кібербезпеки.

Стаття 6. Об'єкти критичної інфраструктури.

Стаття 7. Принципи забезпечення кібербезпеки.

Стаття 8. Національна система кібербезпеки.

Стаття 9. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки.

Стаття 11. Сприяння суб'єктам забезпечення кібербезпеки України.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки.

Стаття 13. Фінансове забезпечення заходів кібербезпеки.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ.

Розглянемо ключові статті Закону, зі змісту яких стає зрозумілою суть діяльності суб'єктів інформаційних відносин (а в контексті положень цього Закону – *суб'єктів забезпечення кібербезпеки*, і ***в першу чергу – ДССЗЗІ***) із забезпечення кібербезпеки в державі.

Загальну модель забезпечення кібербезпеки України на підставі положень Закону можна сформулювати таким чином:

Мета організації кібербезпеки в Україні – *захист життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі* (перший абзац тексту Закону) шляхом своєчасного виявлення, запобігання і нейтралізації реальних і потенційних загроз національній безпеці (ст. 1, визначення поняття *кібербезпека*).

В центрі головних пріоритетів знаходяться *об'єкти кібербезпеки та кіберзахисту (ст. 4).*

*До об'єктів **кібербезпеки** належать:*

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

***5) об'єкти критичної інфраструктури**.*

Об'єктами ***кіберзахисту*** *є:*

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) ***об'єкти критичної інформаційної інфраструктури;***

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Серед ***об'єктів кібербезпеки та кіберзахисту*** особливої уваги потребують ***об'єкти критичної інфраструктури.*** Для таких об'єктів вживаються підвищені заходи забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів, захисту технологічної інформації відповідно до вимог законодавства, невідкладного інформування урядової команди реагування на комп'ютерні надзвичайні події України *CERT-UA* про інциденти кібербезпеки, організації проведення незалежного аудиту інформаційної безпеки із покладанням відповідальності на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури (ст. 6).

З метою реалізації заходів кібербезпеки в державі створена *Національна система кібербезпеки* (ст. 8), яка є сукупністю ***суб'єктів забезпечення кібербезпеки*** *та взаємопов'язаних* ***заходів*** *політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.*

Як бачимо, перелік заходів багатовекторний і стосується різних галузей діяльності держави. Для їхньої організації, впровадження та

контролю повноти та якості виконання залучена ціла низка ***суб'єктів забезпечення кібербезпеки із визначеними Законом повноваженнями.***

Суб'єктами забезпечення кібербезпеки *в Україні є (ст. 5):*

а) *суб'єкти, які забезпечують формування, реалізацію державної політики у сфері кібербезпеки, координацію, контроль за діяльністю суб'єктів сектору безпеки і оборони:*

– Президент України;

– Рада національної безпеки і оборони України (Національний координаційний центр кібербезпеки – робочий орган РНБО);

– Кабінет Міністрів України.

б) *суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки:*

– міністерства та інші центральні органи виконавчої влади (***Державна служба спеціального зв'язку та захисту інформації України***, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи);

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні й контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– військові формування Збройних Сил України, утворені відповідно до закону;

– Національний банк України;

– підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

– суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Перелік *загальних завдань усіх суб'єктів* визначений у положеннях ст. 5. Це:

1) здійснення заходів щодо запобігання використанню кіберпростору з метою воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних дій;

2) виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснення інформаційного обміну щодо реалізованих та потенційних кіберзагроз;

4) розробка та реалізація запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечення проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснення інших заходів із забезпечення розвитку та безпеки кіберпростору.

Окрім загальних завдань, кожний із вищевказаних суб’єктів у межах своєї компетенції виконує покладені на нього конкретні завдання у обсязі визначених у ст. 8 Закону (завдання **ДССЗЗІ**, Національної поліції України, СБУ, МОУ та ГШ ЗСУ, розвід. органів, Національного банку України).

У переліку суб’єктів забезпечення кібербезпеки Національної системи кібербезпеки докладно розглянемо повноваження, які покладено на ***Державну службу спеціального зв’язку та захисту інформації України*** *(с. 8 п. 2 підпункт 1).*

Державна служба спеціального зв’язку та захисту інформації України:

а) забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

б) координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту;

в) забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

г) здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

д) інформує інших суб’єктів про кіберзагрози та відповідні методи захисту від них;

е) забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їхньої атестації (переатестації);

ж) координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

з) забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

В положеннях ст. 9 Закону визначені завдання Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Положеннями п. 3 ст. 8 Закону визначено *шляхи, якими забезпечується функціонування Національної системи кібербезпеки в цілому*. У переліку шляхів *(в контексті завдань даного освітнього компонента)* наголошуємо на підпункті 2):

створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки ***відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО***.

До вимог цього підпункту ми незабаром повернемося, коли йтиметься про інтеграційні процеси нормативно-правових актів України з міжнародними стандартами та вимогами в галузі ІБ на наступному занятті.

У відповідних статтях Закону визначено також механізми впровадження інших важливих організаційних заходів у сфері кібербезпеки, а саме: положення щодо провадження державно-приватної взаємодії у сфері кібербезпеки (ст. 10); сприяння суб'єктам забезпечення кібербезпеки України (ст. 11); відповідальності за порушення законодавства у сфері кібербезпеки (ст. 12) та інші.

Важливою складовою моделі забезпечення кібербезпеки України є ***організація контролю за законністю заходів із забезпечення кібербезпеки держави*** (ст. 15).

Відповідно до положень цієї статті *контроль за дотриманням законодавства* під час ужиття заходів із забезпечення кібербезпеки здійснює ***Верховна Рада України*** в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснює ***Уповноважений Верховної Ради України з прав людини***.

Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснює ***Президент України та Кабінет Міністрів України*** в порядку, визначеному Конституцією і законами України.

Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави ***проводиться щороку*** згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подають Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап'ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, *подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави*, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до повноважень якого належать питання інформатизації та зв'язку, може порушити клопотання про розгляд цих питань Верховною Радою України.

Отже, *Закон України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII є базовим законодавчим актом конституативного рівня, в якому визначені головні правові та організаційні основи забезпечення кібербезпеки держави, та який унаочнює широке коло завдань та повноважень ДССЗЗІ України, складає основу подальшого нормативно-правового упорядкування інших важливих напрямків кіберзахисту та кібербезпеки.*

1.4.2 "Стратегія кібербезпеки України" (указ Президента України від 26 серпня 2021 року № 447/2021)

У загальній ієрархії НПА, чинних у сфері забезпечення кібербезпеки держави, *"Стратегія кібербезпеки України", яка була ухвалена указом Президента України від 26 серпня 2021року № 447/2021 (далі – Стратегія КБУ),* займає наступне місце після законодавчих актів.

В положеннях Стратегії КБУ як важливого документа національного значення із врахуванням загроз та ризиків, пов'язаних із агресією Росії проти нашої держави, ***визначено на 2021-2025 роки головні вектори щодо подальших кроків розбудови національної системи кібербезпеки, впровадження системних заходів щодо надійного захисту національного сегмента кіберпростору, зовнішньополітичної діяльності у сфері посилення кібербезпеки****.* [20]

Загальне призначення Стратегії КБУ визначене на початку НПА у фразі БЕЗПЕЧНИЙ КІБЕРПРОСТІР - ЗАПОРУКА УСПІШНОГО РОЗВИТКУ КРАЇНИ (тобто нормативно-правове обґрунтування пріоритетних цілей, завдань та напрямків діяльності суб'єктів кібербезпеки задля створення безпечного кіберпростору держави як важливої складової успішного розвитку України).

Вимоги *Стратегії КБУ* базуються на положеннях Конституції України, законів України "Про національну безпеку України" та "Про основні засади забезпечення кібербезпеки України", Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність, Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні, затвердженої Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів.

Положення *Стратегії КБУ* сформульовані на 13 сторінках у тексті 9 взаємопов'язаних розділів, в яких детально та послідовно на період 2021-2025 років визначені пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов задля побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Назви розділів розкривають зміст організаційних засад із впровадження заходів з кібербезпеки у такому порядку:

Розділ 1. Кібербезпека: ***глобальний контекст****.*

Розділ 2. Стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96.

Розділ 3. Національний кіберпростір: ***виклики та кіберзагрози****.*

Розділ 4. Національна система кібербезпеки: ***засади розбудови****.*

Розділ 5. ***Пріоритети*** *забезпечення кібербезпеки України та* ***стратегічні цілі****.*

Розділ 6. ***Стратегічні завдання****.*

Розділ 7. ***Напрями зовнішньополітичної діяльності*** *України у сфері кібербезпеки.*

Розділ 8. ***Механізми реалізації*** *стратегії та* ***забезпечення відкритості****.*

Розділ 9. ***Виміри успіху*** *(метрики).*

Положення усіх 9 розділів важливі, тому коротко розглянемо їхню головну сутність.

Розділ 1. Кібербезпека: ***глобальний контекст****.*

З переходом цивілізації планети до активного формування шостого технологічного укладу (для якого характерними показниками є застосування людством сучасних біотехнологій, нанотехнології, систем штучного інтелекту, глобальних інформаційних мереж, інтегрованих високошвидкісних транспортних систем тощо) відбуваються стрімкі зміни у сучасному кіберпросторі, як на національному, так і на транснаціональному рівнях. В глобальному контексті між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їхнє прагнення унаслідок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами стає одним із театрів воєнних дій. Для театру воєнних дій у кіберпросторі, власне, й створені відповідні суб’єкти та категорії: кібервійська, превентивні наступальні операції у кіберпросторі, інформаційно-психологічні операції тощо.

Аналізуючи потоки доступної щоденної інформації, ми переконуємося в наявності такої агресії з боку Росії не тільки на реальних фронтах, а й у кіберпросторі. Сьогодні це є реальною складовою нашого життя.

Зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти й механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси.

Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо.

Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя.

Ці обставини зумовлюють необхідність ухвалення нової Стратегії кібербезпеки України, яка за змістом і буде відповідати цим завданням.

Розділ 2. Стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96.

В другому розділі проведено аналіз щодо впровадження в державі тих фундаментальних заходів щодо становлення та розвитку національної системи кібербезпеки, які були визначені як пріоритетні на період дії *Стратегії кібербезпеки України від 15 березня 2016 року.*

Поряд із позитивними зрушеннями у розвитку національної системи кібербезпеки, в Стратегії КБІ зазначено те, чого не вдалось досягти, а саме:

– діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан реалізації попередньої Стратегії кібербезпеки України за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організація і проведення наукових досліджень у сфері кібербезпеки;

– в державі не було сформовано перелік об'єктів критичної інформаційної інфраструктури;

– не було створено модель державно-приватного партнерства у сфері кібербезпеки;

– розвиток цифрової грамотності здійснювався без чіткої програми, а заходи з кібернавчання проводились епізодично;

– не були чітко сформульовані головні пріоритети та напрямки забезпечення кібербезпеки держави; значна частина із сформульованих не мала зрозумілої кінцевої мети та була неконкретною;

– незадовільним був рівень планування заходів з реалізації положень попередньої *Стратегії КБІ.* Реалізація зазначеної *Стратегії б*ула ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення.

– не були розроблені індикатори виконання попередньої Стратегії КБІ, що ускладнило процес оцінки її результативності та відокремлення незавершених завдань. Участь у реалізації її положень переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучалися заклади освіти та наукові установи.

Цілком зрозумілим є те, що Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

Розділ 3. Національний кіберпростір: ***виклики та кіберзагрози***.

В розділі 3 чітко сформульовані виклики та кіберзагрози, які є надважливими в сучасному кіберпросторі.

Викликами для України у сфері кібербезпеки є:

активне використання кіберзасобів у міжнародній конкуренції;

змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж великих даних, інтернету, речей, штучного інтелекту тощо;

мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;

вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;

упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Загрозами кібербезпеці України є:

Гібридна агресія Російської Федерації проти України в кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів

України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності. Особливостями таких кібератак є їхня тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію.

Кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо.

Використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності.

В цьому розділі також визначені *передумови та чинники*, які формують вищенаведені загрози.

Розділ 4. Національна система кібербезпеки: ***засади розбудови***.

У цьому розділі визначені головні засади розбудови національної системи кібербезпеки на сучасному етапі.

Для подальшої розбудови національної системи кібербезпеки ***на засадах стримування, кіберстійкості, взаємодії*** необхідним є:

посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України в кіберпросторі або, з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними

партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами-членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія).

Україна, крім основних суб'єктів національної системи кібербезпеки, залучить до вирішення завдань у цій сфері ширше коло учасників, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України.

Ключову об'єднувальну та координаційну роль у цьому процесі відіграватиме ***Національний координаційний центр кібербезпеки***.

Україна розбудовуватиме національну систему кібербезпеки, ґрунтуючись на таких ***засадах***:

всеосяжному розумінні та постійному аналізі глобальних трендів кібербезпекового середовища, неухильному захисті національних інтересів України у сфері кібербезпеки;

перманентності (безперервності) заходів з перегляду та уточнення повноважень і відповідальності суб'єктів забезпечення кібербезпеки держави, удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо його актуалізації відповідно до мінливих безпекових умов;

пріоритетності економічного і соціального розвитку суспільства;

збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина;

чіткому визначенні ролей та механізмів взаємодії під час розв'язання завдань кібербезпеки, стимулюванні до обміну інформацією, знаннями і досвідом;

ризик-орієнтованому підході до забезпечення кібербезпеки;

співпраці та інклюзивному діалогу (залучення всіх зацікавлених суб’єктів забезпечення кібербезпеки), зміцненні довіри, зокрема в рамках державно-приватного партнерства;

впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки;

збалансованому розподілі наявних матеріальних, фінансових та інших ресурсів;

проєктивному підході до нейтралізації кіберзагроз;

забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

Розділ 5. ***Пріоритети*** *забезпечення кібербезпеки України та* ***стратегічні цілі.***

Пріоритетами *забезпечення кібербезпеки України є:*

убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

захист прав, свобод і законних інтересів громадян України у кіберпросторі;

європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії.

Головними ***засадами (векторами) трансформування*** національної системи кібербезпеки повинні стати:

формування потенціалу стримування (С) *агресивних намірів проти України інших держав у кіберпросторі;*

забезпечення високого рівня кіберстійкості (К) *національної системи кібербезпеки;*

вдосконалення взаємодії (В) *усіх залучених суб'єктів забезпечення кібербезпеки на національному та міжнародному рівнях.*

Для ***формування потенціалу стримування (С)*** необхідним є досягнення таких ***стратегічних цілей:***

ціль С.1. Дієва кібероборона – Україна створить та забезпечить розвиток (у тому числі кадрово та технологічно) підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі, сформує належну правову, організаційну, технологічну модель їхнього функціонування та застосування, забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їхньої діяльності;

ціль С.2. Ефективна протидія розвідувально-підривній діяльності в кіберпросторі та кібертероризму – Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства й окремих громадян;

ціль С.3. Ефективна протидія кіберзлочинності – Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей

для мінімізації загроз кіберзлочинності, посилення їхнього технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів;

ціль С.4. Розвиток асиметричних інструментів стримування - Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору.

Для набуття кіберстійкості (К) *необхідним є досягнення таких стратегічних цілей:*

ціль К.1. Національна кіберготовність та надійний кіберзахист – Україна запровадить і реалізує чіткі та зрозумілі для всіх зацікавлених сторін заходи щодо національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України. Україна посилить кіберготовність, що полягатиме у здатності всіх зацікавлених сторін, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявляти та усувати передумови до їх виникнення, забезпечивши тим самим кіберстійкість, ***передусім об'єктів критичної інформаційної інфраструктури***. Україна створить національну систему управління інцидентами;

ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки – Україна проведе докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснить заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створення національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним стануть невід'ємними елементами освіти кожного громадянина України;

ціль К.3. Безпечні цифрові послуги – Україна забезпечить досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність та безпеку цифрових послуг протягом усього їхнього життєвого циклу.

<u>Для вдосконалення взаємодії (В)</u> необхідним є досягнення таких стратегічних цілей:

ціль В.1. Зміцнення системи координації – Україна створить умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів, скоординує діяльність усіх зацікавлених сторін задля подолання надзвичайних (кризових) ситуацій у кіберпросторі.

ціль В.2. Формування нової моделі відносин у сфері кібербезпеки – Україна запровадить сервісну модель державної участі в заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки;

ціль В.3. Прагматичне міжнародне співробітництво – Україна спрямує відносини з міжнародними партнерами як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками. Україна забезпечить активну участь у діалозі в рамках міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Забезпечення координації з *міжнародними партнерами здійснюватиметься* ***Міністерством закордонних справ України***.

Розділ 6. ***Стратегічні завдання***

Розбудова національної системи кібербезпеки на засадах ***стримування, кіберстійкості та взаємодії*** *має здійснюватися шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.*

В Стратегії КБУ сформульовані чіткі завдання, спрямовані на досягнення цілей, наведених у попередньому розділі, а саме:

для досягнення цілі С.1 Україна сформує <u>систему дієвої кібероборони</u> шляхом:

утворення в системі Міністерства оборони України кібервійськ та забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору;

запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

розроблення та виконання плану кібероборони як складової частини плану оборони України;

проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав-членів НАТО задля досягнення оперативної сумісності;

створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши на постійних засадах співпрацю з європейською військовою CERT-мережею;

забезпечення оцінки спроможностей суб'єктів сектору безпеки і й оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

запровадження в системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки.

для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності в кіберпросторі та кібертероризму шляхом:

створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури;

удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів;

посилення спроможностей у проведенні негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об'єкти;

посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, спрямованого на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку України у сфері кібербезпеки;

створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності;

вдосконалення нормативно-правового, організаційного та кадрового забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму.

для досягнення цілі С.3 Україна посилить спроможності у протидії кіберзлочинності шляхом:

завершення імплементації в законодавство України положень Конвенції про кіберзлочинність;

врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав-членів ЄС та враховуючи сучасні виклики й тенденції у сфері кібербезпеки;

розроблення концептуальних підходів до реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей);

запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів;

розроблення методики збору кіберстатистики та щорічного оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їхніх офіційних вебсайтах;

розроблення методики проведення щорічних соціологічних досліджень щодо кіберзагроз, з якими стикається населення України, з оцінками ефективності діяльності державних органів у протидії ним і забезпечення проведення таких досліджень;

розроблення методики комунікації між державою та суспільством щодо протидії масштабним кібератакам і кіберінцидентам, створення необхідних умов для її практичної реалізації;

запровадження механізмів ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

врегулювання на законодавчому рівні правового статусу криптовалют;

проведення спільних з ЄС заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози;

забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів;

забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів;

залучення приватних експертів до проведення комп'ютерно-технічних і телекомунікаційних досліджень та експертиз, досліджень програмного забезпечення, які необхідні для швидкого реагування на кіберінциденти та ефективного розслідування кіберзлочинів.

для досягнення цілі С.4 Україна запровадить асиметричні інструменти стримування шляхом:

удосконалення системи розвідувального забезпечення кібербезпеки в частині створення, розвитку сил, засобів та інструментів упередження загроз національній безпеці в кіберпросторі;

посилення заходів щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном;

створення технологічних можливостей підключення постачальниками електронних комунікаційних мереж та/або послуг технічних засобів для здійснення оперативно-розшукових, контррозвідувальних та розвідувальних заходів;

запровадження гармонізованого з євроатлантичною спільнотою підходу до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, розроблення та узгодження з іноземними партнерами механізму спільних дипломатичних та економічних дій і заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність;

застосуванням усіх доступних інструментів дипломатії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України;

налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами-членами ЄС та державами-членами НАТО, створення платформи такого обміну;

врегулювання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі;

розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі.

для досягнення цілі К.1 Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом:

розроблення *Національного плану реагування на надзвичайні (кризові) ситуації в кіберпросторі*, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення;

створення ***національної системи управління інцидентами***, розроблення та впровадження стандартних операційних процедур для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності;

забезпечення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування;

запровадження планування видатків на кібербезпеку за окремими бюджетними програмами;

розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендації з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик;

налагодження на основі взаємної довіри системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи *Національного координаційного центру кібербезпеки*, уніфікації форматів обміну інформацією;

впровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки ***об'єктів критичної інфраструктури та державних органів***, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичної оцінки ризиків на підставі розроблених методик;

впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;

забезпечення розвитку організаційно-технічної моделі кіберзахисту;

завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійного перегляду та оновлення вимог щодо їх кіберзахисту ***з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;***

запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

впровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначення механізмів та базових методик проведення аудитів, встановлення вимог до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;

забезпечення розвитку систем технічного і криптографічного захисту інформації, пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

впровадження вітчизняних рішень із захисту інформації;

проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів;

забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти;

завершення розгортання Національної телекомунікаційної мережі, збільшення її пропускної здатності, передбачення під час її функціонування використання виключно вітчизняних засобів криптографічного захисту інформації;

забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до мережі Інтернет;

створення національного сервісу доменних імен (DNS).

для досягнення цілі К.2 в Україні буде проведено наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кібернавчання для всіх верств населення шляхом:

забезпечення координації наукового співтовариства під час проведення наукових досліджень і розробок у сфері кібербезпеки та залучення його до заходів з реалізації державної політики у сфері кібербезпеки;

визначення довгострокових напрямів проведення досліджень і розробок у сфері кібербезпеки, а також розроблення дієвої програми

державної підтримки (на основі проєктного підходу) стратегічно важливих для кібербезпеки держави наукових установ і організацій, проведення наукових досліджень у цій сфері для потреб національної безпеки і оборони;

забезпечення стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням розвитку новітніх інформаційно-комунікаційних технологій, зокрема, технологій хмарних та квантових обчислень, 5G-мереж, інтернету, штучного інтелекту, а також появи нових засобів реалізації кіберзагроз з метою створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки;

удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки;

розроблення *Загальнонаціональної програми кіберграмотності*, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти;

утворення центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері;

забезпечення матеріального стимулювання фахівців у сфері кібербезпеки, які перебувають на військовій, державній службі, у тому числі на державній службі особливого характеру, службі в правоохоронних органах, або працюють за трудовим договором у державному секторі та безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, з урахуванням рівнів оплати праці таких фахівців у приватному секторі;

залучення суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу.

для досягнення цілі К.3 Україна спрямує *зусилля на забезпечення надійності та безпеки цифрових послуг* шляхом:

зміцнення довіри приватного сектору та громадян до цифрових послуг, які надаються державою, безумовного виконання вимог щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформування громадськості про їхню безпечність та надійність;

впровадження цифрових послуг для населення та розвитку національної інформаційної інфраструктури;

розроблення національних стандартів у сфері кібербезпеки, організаційних та технічних вимог, що стосуються безпеки застосунків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень, *з урахуванням європейських та міжнародних стандартів;*

створення органів з оцінки відповідності надавачів електронних довірчих послуг вимогам для кваліфікованих надавачів кваліфікованих електронних довірчих послуг;

створення необхідних передумов (нормативних, організаційних, технологічних) для автентифікації користувачів сервісів цифрових послуг (там, де це потрібно) за допомогою інтегрованої системи електронної ідентифікації з використанням технологій електронної ідентифікації та/або електронних довірчих послуг;

підвищення ефективності системи захисту персональних даних громадян шляхом гармонізації законодавства України з відповідним законодавством ЄС та посилення відповідальності за порушення встановлених вимог.

для досягнення цілі В.1 Національний координаційний центр кібербезпеки забезпечить скоординовану діяльність усіх зацікавлених сторін у процесі розбудови та функціонування національної системи кібербезпеки шляхом:

розроблення та затвердження порядку проведення огляду національної системи кібербезпеки, забезпечивши його проведення не менше ніж раз на рік протягом реалізації Стратегії;

запровадження обов'язкового негайного, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки;

забезпечення розгляду найважливіших питань у сфері кібербезпеки України на засіданнях Національного координаційного центру кібербезпеки, системного контролю за станом виконання його рішень;

запровадження скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем;

розроблення та запровадження механізмів заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки;

забезпечення щорічного оприлюднення основними суб'єктами національної системи кібербезпеки публічних звітів про стан кібербезпеки за сферами відповідальності.

для досягнення цілі В.2 Україна у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі, шляхом:

врегулювання на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми й методи здійснення

такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проєктів у цій сфері;

запровадження проведення на регулярній основі консультацій зацікавлених сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічного сприяння їхньому розвитку;

залучення на регулярній основі представників наукових установ, громадських організацій та незалежних експертів у сфері кібербезпеки до розроблення проєктів нормативно-правових актів, нормативних документів та стандартів у цій сфері;

підвищення ефективності залучення громадськості до ухвалення рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їхніх результатів на інформаційних ресурсах Національного координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки;

стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно будуть використовуватися для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури;

впровадження програми розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання;

продовження практики щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, закладів освіти та наукових установ, а також громадських об'єднань та приватного сектору;

запровадження системи страхування від кіберризиків, зокрема механізму оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування;

розроблення фінансових та нефінансових механізмів для сприяння впровадженню сучасних технологій кібербезпеки у державному і приватному секторі, включно зі страхуванням, лізингом, пільгами тощо.

для досягнення цілі В.3 Україна *розвиватиме міжнародне співробітництво у сфері кібербезпеки, спрямоване, передусім, на забезпечення незалежності й державного суверенітету, відновлення територіальної цілісності України, шляхом:*

забезпечення участі України у міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі;

забезпечення участі України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та

гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах;

розширення шляхом діалогу з міжнародними партнерами доступу правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу I-24/7;

продовження співробітництва з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки, зокрема з питань скоординованого розкриття вразливостей та імплементації Директиви Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як елемента євроінтеграції України;

поглиблення співпраці з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій, зокрема з питань стандартизації у цих сферах;

поглиблення співпраці з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства;

розвитку міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України;

продовження практики проведення двосторонніх кібердіалогів з державами-партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між зацікавленими державними органами України та іноземних держав, розширення кола держав-партнерів, з якими проводяться кібердіалоги, ініціювання питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки;

створення постійної робочої групи з питань взаємодії з провідними IT-компаніями, світовими провайдерами цифрових послуг, соціальними мережами з метою протидії гібридним загрозам, поширенню дезінформації, можливості застосування санкцій відповідно до законів України;

визначення та затвердження переліку пріоритетних напрямів залучення міжнародної технічної допомоги у сфері кібербезпеки України.

*Розділ 7. Напрями **зовнішньополітичної діяльності** України у сфері кібербезпеки.*

Україна у сфері кібербезпеки ***забезпечить поглиблення євроінтеграційних процесів*** шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з упровадженими практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів,

спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Україна приділятиме особливу увагу спільній з партнерами ***протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства,*** іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти, розвиватиме на договірній основі з партнерськими спецслужбами держав-членів ЄС і держав-членів НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовуватиме кращі світові практики, активно здійснюватиме інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки.

Україна ***співпрацюватиме з міжнародними партнерами, організаціями та іншими зацікавленими сторонами, які поділяють наше спільне бачення майбутнього кіберпростору як глобального, відкритого, вільного, стабільного та безпечного,*** в основі якого дотримання прав людини, основних свобод та демократичних цінностей, що є запорукою соціально-економічного та політичного розвитку України.

Україна ***продовжить активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН,*** а також норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації зацікавлених сторін на міжнародних форумах, в яких Україна буде не лише учасником, а й ініціатором та організатором.

Україна ***максимально підтримуватиме мультистейк- холдерську (багатосторонню) модель управління інтернетом, сприяючи міжнародним, регіональним та національним дискусіям з цього питання, залученню до цього процесу представників приватного сектору, наукових та освітніх кіл, інститутів громадянського суспільства.*** Спроби окремих авторитарних держав суверенізувати інтернет суперечать довгостроковим інтересам України та її моделі соціально-економічного розвитку.

Україна буде ***сприяти подальшому дотриманню міжнародного права та стандартів у сфері прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями.*** Для цього Україна активізує свою участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширить представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері.

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури інтернету Україна виходить з того, що інтернет має залишатися глобальним та відкритим, технології повинні орієнтуватися на людину, її базові свободи, гарантувати невтручання в її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження повинні здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним. Водночас у зв'язку з ускладненням міжнародної безпеки в кіберпросторі Україна займатиме активнішу позицію в дискусіях ООН та інших міжнародних форумах для просування, координації та консолідації її позиції у сфері кібербезпеки, зменшуючи небезпеку мілітаризації кіберпростору.

Україна ***розвиватиме мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати й механізми міжнародного співробітництва.***

Розділ 8. ***Механізми реалізації стратегії та забезпечення відкритості***

Координатором реалізації цієї Стратегії є робочий орган Ради національної безпеки і оборони України - ***Національний координаційний центр кібербезпеки.***

Реалізація Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

Основним ***критерієм результативності*** *Стратегії є досягнення мети та стратегічних цілей шляхом виконання визначених стратегічних завдань.*

Національний координаційний центр кібербезпеки у визначених законодавством формах забезпечує (на весь період дії Стратегії) планування реалізації Стратегії, координує і контролює стан її виконання та ефективність.

План реалізації Стратегії, розроблений Національним координаційним центром кібербезпеки та затверджений в установленому порядку, є основою для щорічного планування суб'єктами забезпечення кібербезпеки заходів з реалізації Стратегії.

Кабінет Міністрів України в установленому порядку забезпечує необхідними силами, засобами і ресурсами виконання заходів з реалізації Стратегії.

Результати виконання запланованих заходів з реалізації Стратегії подаються суб'єктами забезпечення кібербезпеки до Національного координаційного центру кібербезпеки.

Ефективність реалізації Стратегії визначається у проведених у встановленому порядку оглядах стану:

національної системи кібербезпеки;

кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Результати оглядів можуть стати підставою для внесення змін до Плану реалізації Стратегії та/або щорічних планів заходів з реалізації Стратегії, що обумовлено необхідністю адаптації до змін у безпековому середовищі, усунення та мінімізації негативних тенденцій у сфері кібербезпеки.

Стратегія є основою для обґрунтування розподілу необхідних для забезпечення кібербезпеки матеріальних, кадрових та інших ресурсів.

Фінансування заходів з реалізації Стратегії здійснюватиметься в межах видатків, передбачених Державним бюджетом України та з інших джерел, не заборонених законодавством.

У порядку координації ***Національний координаційний центр кібербезпеки*** під час підготовки матеріалів до засідань Ради національної безпеки і оборони України щодо проєкту Закону України про Державний бюджет України та пропозицій до Бюджетної декларації за статтями, пов'язаними із забезпеченням національної безпеки і оборони України, аналізує пропозиції суб'єктів забезпечення кібербезпеки України щодо фінансування заходів з кібербезпеки, передбачених положеннями Стратегії кібербезпеки України, та надає відповідні пропозиції.

Згідно із законодавством державні органи, підприємства, установи та організації передбачатимуть у своїх планах фінансові витрати на кібербезпеку. У рамках державно-приватного партнерства, міжнародної технічної допомоги залучатимуться інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки.

Щороку Національний координаційний центр кібербезпеки оприлюднює публічний звіт про стан реалізації Стратегії за загальними оцінками.

Процес реалізації Стратегії має бути максимально прозорим, відкритим та супроводжуватися ***демократичним цивільним контролем***. З цієї метою основними суб'єктами національної системи кібербезпеки в межах компетенції додатково буде здійснюватися щорічне інформування громадськості через власні офіційні веб-сайти про стан реалізації ними Стратегії та стан фінансування відповідних заходів.

Розділ 9. ***Виміри успіху (метрики)***

Ефективність реалізації Стратегії буде визначатися через постійний моніторинг її виконання та спиратися на чітку ***систему індикаторів стану кібербезпеки,*** які буде розроблено протягом першого року реалізації Стратегії.

Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації Стратегії з таких питань, як:

виконання стратегічних завдань у межах цілей, визначених Стратегією (за кожним завданням);

досягнення стратегічних цілей, визначених Стратегією (за кожною ціллю);

рівень впливу заходів, що здійснюються в межах Стратегії, на національну систему кібербезпеки та цифрову трансформацію держави.

Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства й держави. Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за такими ***критеріями:***

рівень довіри населення до держави щодо безпечності кіберпростору;

формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки, крім державних інституцій, залучені приватні суб'єкти та громадяни;

рівень захищеності національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією Російської Федерації проти України).

За допомогою розгалуженої системи індикаторів буде визначатися стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави.

Система індикаторів буде включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії.

Україна розвиватиме національний кіберпростір як глобальний, відкритий, вільний, стабільний та безпечний задля захисту суверенітету держави, соціального і економічного розвитку суспільства.

За результатами реалізації Стратегії Україна у співпраці з приватним сектором та із залученням міжнародних партнерів забезпечить *(очікувані результати щодо досягнення головних цілей та завдань, сформульованих у Стратегії КБУ):*

стійкість до кіберзагроз, підвищивши здатність державних органів, бізнесу й громадян захищати себе та реагувати на кіберзагрози;

спроможність до ефективної протидії недружнім діям у кіберпросторі, забезпечивши їх швидке виявлення та розслідування, створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі;

розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам.

В центрі головних пріоритетів кібербезпеки держави відповідно до положень Стратегії КБУ, а також ст. 4 Закону України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII знаходяться об'єкти кібербезпеки та кіберзахисту, серед яких особливої уваги потребують ***об'єкти критичної інфраструктури та їхні комунікаційні (технологічні системи)*** *(далі – об'єкти критичної інформаційної інфраструктури),* кібератака на які безпосередньо вплине на стале функціонування об'єктів критичної інфраструктури в цілому. У сфері відповідальності Державної служби спеціального зв'язку та захисту інформації України знаходяться завдання щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури таких об'єктів, а також координація діяльності інших суб'єктів забезпечення кібербезпеки щодо їх кіберзахисту *(ст. 8, п. 2 Закону України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII).*

Отже, "Стратегія кібербезпеки України" (ухвалена указом Президента України від 26 серпня 2021 року № 447/2021) є фундаментальним НПА держави, в якому, із врахуванням загроз та ризиків у кіберпросторі, пов'язаних з агресією Росії проти нашої держави, на період 2021-2025 років визначено головні вектори щодо подальших кроків розбудови національної системи кібербезпеки, сформульовано пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов задля побудови безпечного функціонування кіберпростору держави, його використання в інтересах особи, суспільства й держави.

Одним із найважливіших пріоритетів у цьому секторі ІБ є забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури, а також координація діяльності інших суб'єктів забезпечення кібербезпеки щодо

кіберзахисту таких об'єктів. Це важливе завдання в сучасних умовах покладається на фахівців Державної служби спеціального зв'язку та захисту інформації України.

Вище сформульовані положення зобов'язують розглянути зміст таких законодавчих та нормативно-правових актів України, як Закон України "Про критичну інфраструктуру" від 18 жовтня 2022 року № 2684-IX (зі змінами й доповненнями) та "Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури" (постанова КМУ від 19 червня 2019 року № 518).

1.4.3 Закон України "Про критичну інфраструктуру" від 18 жовтня 2022 року № 2684-IX (зі змінами й доповненнями)

Закон України "Про критичну інфраструктуру" від 18 жовтня 2022 року № 2684-IX (зі змінами й доповненнями) визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. [21]

Закон є базовим, він регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час.

Особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України "Про правовий режим воєнного стану", "Про правовий режим надзвичайного стану", "Про функціонування єдиної транспортної системи України в особливий період" та "Про оборону України".

Зміст Закону складається із шести розділів:

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ (ст. ст. 1-3);

Розділ II. ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (ст .ст. 4-7);

Розділ III. КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ (ст. ст. 8-12);

Розділ IV. НАЦІОНАЛЬНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (ст. ст. 13-21);

Розділ V. ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (ст. ст. 22-32);

Розділ VI. ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ (п. п. 1-11).

З'ясуємо важливі для фахівців ДССЗЗІ положення статей Закону.

У Розділі І. ЗАГАЛЬНІ ПОЛОЖЕННЯ:

У ***Ст. 1. Визначення основних термінів*** наведені визначення двадцяти чотирьох важливих термінів, які надають можливості однозначного тлумачення вимог положень статей Закону.

Доцільно запам’ятати визначення наступних найчастіше вжитих у тексті Закону термінів:

безпека критичної інфраструктури *– стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;*

захист критичної інфраструктури *– всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;*

категоризація об'єктів інфраструктури *– віднесення об'єктів інфраструктури до категорій критичності об'єктів інфраструктури;*

категорія критичності (критерії) об'єкта критичної інфраструктури *– ступінь (відносний рівень) важливості об'єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг;*

критична технологічна інформація *– дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури;*

Національна система захисту критичної інфраструктури *– сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;*

об'єкти критичної інфраструктури *– об'єкти інфраструктури, системи, їхні частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;*

стійкість критичної інфраструктури *– стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду.*

У ***Ст. 2. Законодавство про критичну інфраструктуру та її захист*** наведений перелік законодавчих, нормативно-правових актів та міжнародних договорів України, що складають законодавство про критичну інфраструктуру та її захист.

Стаття 3. Сфера застосування цього Закону містить положення відповідно до заголовку статті.

Зміст **Розділу ІІ. ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ** структурований у таких статтях та положеннях:

Стаття 4. Засади державної політики у сфері захисту критичної інфраструктури.

Стаття 5. Мета та завдання державної політики у сфері захисту критичної інфраструктури.

Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їхнє функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури.

В цій статті визначені *головні завдання* щодо формування і реалізації державної політики у сфері захисту критичної інфраструктури.

Стаття 6. Основні принципи функціонування національної системи захисту критичної інфраструктури.

Стаття 7. Рівні управління національною системою захисту критичної інфраструктури.

1. Національна система захисту критичної інфраструктури має такі рівні управління:

1) ***загальнодержавний рівень,*** управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з цим Законом, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

2) ***регіональний та галузевий рівні,*** управління на яких здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

3) ***місцевий рівень***, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них цим Законом;

4) ***об'єктовий рівень***, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

Розділ ІІІ. КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Віднесення об'єктів до критичної інфраструктури.

Стаття 9. Сектори критичної інфраструктури.

Для організації ефективного забезпечення безпеки й стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури.

Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури.

Перелік секторів критичної інфраструктури та суб'єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, ***визначається Кабінетом Міністрів України***.

До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;
2) енергозабезпечення (у тому числі постачання теплової енергії);
3) водопостачання та водовідведення;
4) продовольче забезпечення;
5) охорона здоров'я;
6) фармацевтична промисловість;
7) виготовлення вакцин, стале функціонування біолабораторій;
8) інформаційні послуги;
9) електронні комунікації;
10) фінансові послуги;
11) транспортне забезпечення;
12) оборона, державна безпека;
13) правопорядок, здійснення правосуддя, тримання під вартою;
14) цивільний захист населення та територій, служби порятунку;
15) космічна діяльність, космічні технології та послуги;
16) хімічна промисловість;
17) дослідницька діяльність.

Стаття 10. Категоризація об'єктів критичної інфраструктури.

Для визначення рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури відповідно до рівня їхньої важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури ***здійснюється категоризація об'єктів критичної інфраструктури*** відповідно до категорій критичності, визначених цим Законом.

Установлюються такі категорії критичності об'єктів критичної інфраструктури:

1) ***І категорія критичності*** – особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) ***ІІ категорія критичності*** – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) ***ІІІ категорія критичності*** – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) ***IV категорія критичності*** – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Категоризація об'єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

4. Секторальні органи разом з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об'єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України, а в банківській та фінансовій системах – Національним банком України, у сферах, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, - такими державними органами.

Стаття 11. Реєстр об'єктів критичної інфраструктури.

Для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури формується ***Реєстр об'єктів критичної інфраструктури.***

В статті встановлено порядок створення, ведення та користування Реєстром посадовими особами різних суб’єктів національної системи захисту критичної інфраструктури.

Стаття 12. Паспортизація об'єктів критичної інфраструктури.

З метою проведення аналізу можливих основних загроз та потенційних негативних наслідків для об'єктів критичної інфраструктури, запобігання та попередження виникнення таких загроз для критичної інфраструктури оператори об'єктів критичної інфраструктури готують і подають на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, відповідного функціонального органу ***паспорт безпеки на кожний об'єкт критичної інфраструктури***.

Паспорт безпеки на об'єкт критичної інфраструктури містить інформацію про ідентифікацію об'єкта та заходи щодо його захисту і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв'язок та обмін інформацією з суб'єктами національної системи захисту критичної інфраструктури.

В статті визначений порядок розробки Паспорту безпеки та встановлена відповідальність операторів критичної інфраструктури за достовірність даних, наведених у паспорті безпеки, а також своєчасність внесення до нього змін.

Розділ IV. НАЦІОНАЛЬНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 13. Формування та реалізація державної політики у сфері захисту критичної інфраструктури.

Кабінет Міністрів України забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури***, визначає уповноважений орган*** з питань захисту критичної інфраструктури України.

Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб'єктів національної системи захисту критичної інфраструктури.

В положеннях статті встановлено порядок обміну необхідною інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури.

Стаття 14. Суб'єкти національної системи захисту критичної інфраструктури.

В даній статті Закону встановлений перелік суб'єктів національної системи захисту критичної інфраструктури України. До переліку включено:

1) Кабінет Міністрів України;

2) Апарат Ради національної безпеки і оборони України;

3) Центральна виборча комісія;

4) Національний банк України;

5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

6) ***Адміністрація Державної служби спеціального зв'язку та захисту інформації України;***

7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом;

8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту;

10) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади;

11) Служба безпеки України;

12) правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності;

13) Збройні Сили України, інші військові формування, утворені відповідно до законів України;

14) місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення);

15) органи місцевого самоврядування;

16) оператори критичної інфраструктури;

17) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Стаття 15. Режими функціонування національної системи захисту критичної інфраструктури.

Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

1) ***штатний режим*** – суб'єктами національної системи захисту критичної інфраструктури стосовно оцінки можливих загроз та інформування щодо них. *Функціонування інфраструктури здійснюється відповідно до проєктного цільового призначення*;

2) ***режим готовності та запобігання реалізації загроз*** – секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози.

Функціонування інфраструктури здійснюється відповідно до проєктного цільового призначення;

3) ***режим реагування на виникнення кризової ситуації*** – суб'єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. *Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступ до об'єктів;*

4) ***режим відновлення штатного функціонування*** – суб'єктами національної системи захисту критичної інфраструктури: застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму. *Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.*

З врахуванням того, що певні режими функціонування вводяться різними суб'єктами національної системи захисту критичної інфраструктури, цими суб'єктами розробляється план взаємодії з іншими суб'єктами, який затверджується Кабінетом Міністрів України і переглядається раз на три роки.

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури України.

Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об'єктів критичної інфраструктури.

Діяльність уповноваженого органу у сфері захисту критичної інфраструктури України спрямовує, координує та контролює Кабінет Міністрів України.

В статті визначені функції уповноваженого органу у сфері захисту критичної інфраструктури.

Стаття 17. Функціональні органи у сфері захисту критичної інфраструктури.

В статті визначені повноваження ***функціональних органів у сфері захисту критичної інфраструктури*** (органів державної влади, визначених відповідальними за функціонування окремих державних систем захисту та реагування).

Стаття 18. Особливості діяльності окремих органів, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури.

Стаття 19. Секторальні органи у сфері захисту критичної інфраструктури.

В статті визначені завдання ***секторальних органів у сфері захисту критичної інфраструктури*** (державних органів, визначених відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури).

Стаття 20. Місцеві органи виконавчої влади та військово-цивільні адміністрації.

В статті визначені завдання місцевих органів виконавчої влади та військово-цивільних адміністрацій у сфері захисту критичної інфраструктури.

Стаття 21. Завдання, права та обов'язки операторів критичної інфраструктури.

Розділ V. ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 22. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури.

В статті визначено відповідальних суб’єктів, а також порядок розробки та затвердження ***Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури, галузевих, регіональних планів та програм з протидії загрозам критичній інфраструктурі (в тому числі й аварійних планів, планів реагування на кризові ситуації, планів взаємодії, планів відновлення об'єктів критичної інфраструктури, планів проведення навчань та тренувань).***

Стаття 23. Здійснення моніторингу рівня безпеки об'єктів критичної інфраструктури.

В статті встановлено періодичність та порядок моніторингу *(шляхом проведення оцінки стану захищеності об'єктів критичної інфраструктури)* ***секторальними та функціональними органами*** у сфері захисту критичної інфраструктури відповідно до їхніх повноважень.

Стаття 24. Взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки.

В статті визначено порядок взаємодії національної системи захисту критичної інфраструктури з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах, з національною системою кібербезпеки, з об'єднаною цивільно-військовою системою організації повітряного руху України, з єдиною державною системою цивільного захисту, з правоохоронними органами у сфері протидії злочинності, з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки, з іншими системами захисту важливих державних об’єктів та інформаційних ресурсів.

Стаття 25. Державно-приватне партнерство у сфері захисту критичної інфраструктури.

В статті визначено шляхи здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури (обмін необхідною інформацією між суб’єктами, створення системи підготовки кадрів в цій сфері, залучення експертного потенціалу наукових установ, професійних, громадських об'єднань до підготовки галузевих проєктів та нормативно-правових актів, організації системи оповіщення населення та суб'єктів господарювання про інциденти та кризові ситуації на об'єктах критичної інфраструктури тощо).

Стаття 26. Проведення незалежного аудиту діяльності національної системи захисту критичної інфраструктури.

Незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України здійснюється *шляхом проведення щорічного зовнішнього аудиту його діяльності*. Зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України проводиться ***Рахунковою палатою***.

Стаття 27. Парламентський контроль у сфері захисту критичної інфраструктури.

Контроль за дотриманням законодавства під час проведення заходів із забезпечення захисту критичної інфраструктури ***здійснює Верховна Рада України*** в порядку, визначеному Конституцією України. Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, *та* ***комітет Верховної Ради України***, до предмета відання якого належать питання кібербезпеки об'єктів критичної інформаційної інфраструктури, на своїх засіданнях розглядають звіт

уповноваженого органу у сфері захисту критичної інфраструктури України про результати незалежного аудиту діяльності щодо ефективності системи забезпечення захисту критичної інфраструктури.

Стаття 28. Громадський нагляд у сфері захисту критичної інфраструктури.

Право громадського нагляду у сфері захисту критичної інфраструктури реалізується громадянами України ***через громадські об'єднання***, членами яких вони є, ***через депутатів місцевих рад, особисто шляхом звернення*** до Уповноваженого Верховної Ради України з прав людини або до державних органів у порядку, встановленому Конституцією України, Законом України "Про громадські об'єднання" та іншими законами України, участі в діяльності громадських рад при органах, що формують та забезпечують реалізацію державної політики у сфері забезпечення захисту критичної інфраструктури, проведення незалежного аудиту їхньої діяльності, право доступу до публічної частини звіту щодо забезпечення захисту об'єктів критичної інфраструктури.

Стаття 29. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури.

Особи, винні в порушенні законодавства у сфері захисту критичної інфраструктури, *несуть відповідальність згідно із законом*.

Стаття 30. Фінансування заходів у сфері захисту критичної інфраструктури.

Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти операторів критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 31. Міжнародне співробітництво у сфері захисту критичної інфраструктури.

Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері захисту критичної інфраструктури з іноземними державами, їхніми правоохоронними органами й спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною злочинністю та тероризмом.

Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках

заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".

Відповідно до законодавства у сфері зовнішніх зносин суб'єкти національної системи захисту критичної інфраструктури у межах своїх повноважень здійснюють міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

Стаття 32. Страхування ризиків.

Оператор критичної інфраструктури зобов'язаний забезпечити ***страхування ризику*** настання кризової ситуації.

Перелік об'єктів критичної інфраструктури, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об'єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами) затверджуються Кабінетом Міністрів України, а щодо об'єктів критичної інфраструктури у сфері фінансових послуг – погоджуються з Національним банком України.

Розділ VI. ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

В цьому розділі визначені терміни набрання чинності положень Закону, наведений перелік законодавчих актів України, які потребують змін у зв’язку із виданням даного Закону, а також зміст змін відповідних статей та пунктів.

Отже, Закон України “Про критичну інфраструктуру” від 18 жовтня 2022 року № 2684-IX (зі змінами й доповненнями) є важливим законодавчим актом конститутивного рівня у сфері національної безпеки держави. Він визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури; перелік, повноваження та завдання суб’єктів національної системи захисту критичної інфраструктури; встановлює порядок планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури, здійснення моніторингу рівня безпеки об'єктів критичної інфраструктури, незалежного аудиту діяльності національної системи захисту критичної інфраструктури, парламентського та громадського контролю у сфері захисту критичної інфраструктури; встановлює відповідальність суб’єктів за порушення законодавства у сфері захисту критичної інфраструктури.

Положення Закону є законодавчою основою для подальшого вдосконалення системи нормативно-правового забезпечення у сфері захисту критичної інфраструктури держави.

1.4.4 “Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури” (постанова КМУ від 19 червня 2019 року № 518)

На підставі знань, отриманих під час вивчення попередніх законодавчих актів конститутивного рівня, нам стали відомі основні нормативно-правові засади, цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження суб’єктів забезпечення кібербезпеки в державі, основні засади координації їхньої діяльності у цій сфері, головними напрямками розбудови національної системи кібербезпеки з метою створення передумов задля побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. В цих законодавчих актах визначена важливість ***об’єктів критичної інфраструктури***, як одного із головних об’єктів кіберзахисту держави. На державному рівні сформульоване загальне завдання щодо необхідності впровадження відносно цих важливих об’єктів відповідних заходів кіберзахисту.

Закономірно виникають питання щодо впровадження заходів кіберзахисту на об’єктах критичної інфраструктури держави. І цих питань виникає багато, коли справа доходить до їх практичного впровадження, а саме: які заходи потрібно впроваджувати; хто конкретно несе відповідальність за їх реалізацію, які структурні підрозділи установ є виконавцями цих заходів, які матеріальні, фінансові ресурси та з яких джерел залучаються, і цей перелік питань можна продовжувати далі.

Відповіді на ці питання суто практичної орієнтації покликані надати документи інституційного рівня.

У нашому конкретному випадку – це НПА інституційного рівня ***“Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури” (введено в дію постановою КМУ від 19 червня 2019 року № 518).***

На прикладі цього документа з’ясуємо відмінності у призначенні, побудові та наповненні змістовної частини НПА інституційного рівня порівняно з НПА конститутивного рівня.

Докладніше розглянемо призначення, побудову та наповнення змістовної частини цього документа.

Головною особливістю даного НПА є те, що окрім основної частини тексту, документ містить Додаток.

Основна частина тексту обсягом 5 друкованих аркушів складається із 14 статей. Додаток обсягом 12 сторінок (шрифт 12) є збірником окремих тематичних положень, у яких викладені вимоги до змісту практичних заходів щодо організації та забезпечення кіберзахисту об’єктів критичної інфраструктури. [22]

<u>У основній частині НПА</u>

визначені організаційно-методологічні умови та вимоги кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури.

Для однозначно правильного сприйняття положень НПА введені тлумачення та пояснення щодо основних термінів та понять, які використовуються в документі (ст. ст. 1, 2).

В наступних статтях НПА системно викладені вимоги щодо послідовності впровадження, змісту заходів з організації кіберзахисту об’єктів критичної інфраструктури:

ст. 3. Кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури ***комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю***.

ст. 4. Кіберзахист об’єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Заходи з кіберзахисту передбачені та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

ст. 5. Кіберзахист об’єкта критичної інфраструктури ***забезпечується власником та/або керівником об’єкта критичної інфраструктури*** відповідно до цих Загальних вимог та законодавства у сфері захисту інформації та кібербезпеки.

ст. 6. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури ***комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи у сфері технічного захисту інформації***.

Створення комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

ст. 7. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних

вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури.

Створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог *технічного завдання на створення системи інформаційної безпеки*.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються у звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури ***є стандарт ДСТУ ISO/IEC 27005.***

Власник та/або керівник об’єкта критичної інфраструктури організовує *проведення незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури* згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

ст. 8. Власник та/або керівник об’єкта критичної інфраструктури організовує *невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA* (у разі наявності – галузевої команди реагування на комп’ютерні надзвичайні події), а також *функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ* (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

ст. 9. Державні органи отримують доступ до Інтернету *через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту*, через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-комунікаційні системи закордонних дипломатичних установ України.

ст. 10. Власник та/або керівник об’єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує *створення резервних копій інформаційних ресурсів об’єкта критичної інформаційної інфраструктури* та критичних бізнес/операційних процесів об’єкта критичної інфраструктури для

оперативного їх відновлення у разі пошкодження або знищення.

Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

ст. 11. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту ***використовують ресурси Національної телекомунікаційної мережі.***

ст. 12. Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні забезпечувати:

формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

доступність та відмовостійкість компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної

інфраструктури, наведено ***у Додатку.***

Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури може бути доповнено відповідно до технології обробки інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, особливостей функціонування та програмно-апаратного складу об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, складу інформаційних ресурсів та компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які підлягають захисту, тощо.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури для кожної загрози об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури ***передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури***. У разі коли перелік мінімальних заходів не дає можливості забезпечити блокування (нейтралізацію) усіх загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

Формування додаткових заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури розробник комплексної системи захисту інформації (системи інформаційної безпеки) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

ст. 13. У разі відсутності можливості виконання окремих вимог із забезпечення кіберзахисту, наведених у додатку, і/або неможливості їх застосування до окремих об'єктів захисту чи користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, у тому числі внаслідок їхнього можливого негативного впливу на функціонування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або неможливості їх здійснення на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури через особливості функціонування, або відсутності складу компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури ***повинні бути розроблені й упроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, або обґрунтовано виключені окремі вимоги з переліку базових вимог із***

забезпечення кіберзахисту об'єктів критичної інфраструктури.

Власник та/або керівник об'єкта критичної інфраструктури під час розроблення організаційних і технічних заходів щодо забезпечення кіберзахисту об'єкта критичної інфраструктури обґрунтовує застосування компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури. Водночас під час проведення незалежного аудиту інформаційної безпеки об'єкта критичної інфраструктури або державної експертизи комплексної системи захисту інформації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та зменшення ризиків об'єкта критичної інфраструктури, або обґрунтованість виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури оформлюється окремим рішенням за підписом власника та/або керівника об'єкта критичної інфраструктури.

ст. 14. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єктів критичної інфраструктури, які належать до сфери їхнього управління. ***Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв'язку.***

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов'язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

<u>У Додатку</u>

наведений збірник окремих тематичних положень під загальним заголовком *Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури.*

В ньому викладені технічні та технологічні вимоги до змісту відповідних заходів щодо забезпечення кіберзахисту об'єктів критичної інфраструктури *за певною тематикою за такими розділами*:

Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

Управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Реєстрація подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит.

Забезпечення мережевого захисту компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Визначення умов використання програмного та апаратного забезпечення об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Визначення умов розміщення компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Назви розділів абсолютно однозначно орієнтують нашу свідомість на ***суто практичну направленість вимог, викладених у кожному розділі Додатку.***

Отже, положення розглянутих вище НПА інституційного рівня мають спрямованість на практичне покрокове виконання вимог щодо забезпечення кібербезпеки в певних установах та організаціях. Саме в їхній практичній спрямованості полягає головна відмінність їх призначення порівняно з НПА концептуального та конститутивного рівнів ієрархії. Вони є певною ланкою в системі НПА, на положеннях яких ґрунтуються вимоги інших нормативних документів суто практичного застосування, а саме: методик, правил, інструкцій, порядків, методичних вказівок, рекомендацій тощо.

Зміст та методики практичного виконання вимог цієї низки НПА та нормативних документів, чинних у секторі кібербезпеки держави, будуть докладно вивчатися під час опанування матеріалу освітніх компонент "Кібербезпека", "Аналіз і моніторинг кібербезпеки", "Технології захисту інформації в інформаційно-комунікаційних системах".

1.5 Інтеграційні процеси нормативно-правових актів України з міжнародними стандартами та вимогами в галузі ІБ

1.5.1 Міжнародні стандарти та вимоги в галузі ІБ. Стандарти ЄС

В останнє десятиріччя суттєвий вплив на реалізацію національних інтересів і зовнішньополітичних пріоритетів нашої країни здійснюють загальні тенденції розвитку світового геополітичного процесу, який характеризується загостренням протистояння між країнами демократичного розвитку та країнами із тоталітарною системою правління. Особливо активної динаміки це протистояння набуло із повномасштабною агресією Росії проти нашої держави, яка ще із часів Помаранчевої Революції Гідності остаточно визначилася зі своїм вибором бути в родині країн демократії.

Ці прагнення українського суспільства закріплено в головних концептуальних НПА держави: Законі України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII, "Концепції національної безпеки України", схваленої постановою Верховної Ради України від 16 січня 1997 року № 3/97-ВР, (зі змінами), "Стратегії національної безпеки України", введеної в дію указом Президента України від 26 травня 2015 року, "Доктрині інформаційної безпеки України", введеної в дію указом Президента України від 25 лютого 2016 року № 47/2017, "Стратегії інформаційної безпеки", введеної в дію указом Президента України від 28 грудня 2021 року № 685/2021, та інших, положення яких були розглянуті вище.

Відповідно до положень цих НПА Україна вибрала шлях потужного просування до повноправної участі в загальноєвропейській та регіональній системах колективної безпеки, набуття членства у Європейському Союзі та Організації Північноатлантичного договору, активної участі у міжнародних проєктах миротворчої діяльності під егідою ООН та ОБСЄ.

На сьогоднішній день приєднання України до цих міжнародних політичних та воєнно-політичних інституцій розглядається як реальний цілеспрямований та динамічний процес, який передбачає проведення в нашій державі цілої низки реформ та трансформацій суспільства в багатьох сферах діяльності, зокрема й у сферах інформаційних відносин та інформаційної безпеки держави.

Ці процеси є цілком зрозумілими та очевидними з точки зору здорової логіки: для того, щоб увійти в союз країн, які поділяють спільні цінності – дотримання принципів демократії, верховенства права, гарантій прав та свобод громадян, нетерпимість до корупційних проявів у будь-яких сферах життя тощо – потрібно цілком відповідати цим критеріям та вимогам. Тому на законодавчому та нормативно-правовому рівні у різних сферах

функціонування суспільства необхідно досягти максимального наближення до вимог та норм, які є загальноприйнятними для усіх країн-членів ЄС та НАТО.

У сферах інформаційних відносин та інформаційної безпеки наша держава йде шляхом максимального наближення вимог вітчизняного нормативно-правового забезпечення до положень міжнародних стандартів в цій сфері.

1.5.2 Методичні рекомендації щодо вивчення базових міжнародних стандартів в сфері ІБ

Враховуючи вище зазначене, доцільно в межах групового (практичного) заняття вивчити положення базових міжнародних стандартів, чинних у сфері інформаційної безпеки країн Європейського Союзу, а саме:

міжнародного стандарту ISO/IEC 27001 “Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги” *(далі – міжнародний стандарт ISO/IEC 27001)*;

міжнародного стандарту ISO/IEC 27002 “Інформаційні технології – Методи захисту – Звід практик щодо заходів інформаційної безпеки” *(далі – міжнародний стандарт ISO/IEC 27002);*

міжнародного стандарту ISO/IEC 9798-1:2002 “Інформаційні технології. Методи захисту. Автентифікація суб’єктів (Частина 1. Загальні положення)” *(далі – міжнародний стандарт ISO/IEC 9798-1:2002);*

міжнародного стандарту ISO/IEC 9798-3:2002 “Інформаційні технології. Методи захисту. Автентифікація суб’єктів” (Частина 3. Механізми з використання методу цифрового підпису)” *(далі – міжнародний стандарт ISO/IEC 9798-3:2002)*. [23 - 26]

Під час цього заняття викладач організовує засвоєння здобувачами вищої освіти головних положень НПА шляхом виконання ними спеціально сформульованих завдань. Викладач сприяє формуванню у здобувачів умінь і навичок системного накопичення необхідних професійних знань з метою їх практичного застосування у подальшій службі. У процесі роботи здобувачів викладач контролює вивчення ними головних положень НПА, задає контрольні питання, оцінює відповіді, заохочує їхню активність. У разі запитань з боку здобувачів, надає відповіді та пояснення, наводить наочні приклади.

Пропонуємо такий обсяг завдань щодо вивчення призначення та головних положень НПА під час групового (практичного) заняття, а також

переліки питань для проведення контролю (самоконтролю) якості вивчення матеріалу.

Міжнародний стандарт ISO/IEC 27001 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги"

Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний із іншими стандартами цієї групи (наприклад, з ISO/IEC 27002).

Цей міжнародний стандарт адаптований в системі НПА, чинний у сфері інформаційної безпеки України, з метою визначення єдиних (із державами ЄС) вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) організації.

Обсяг завдань щодо роботи з положеннями міжнародного стандарту ISO/IEC 27001:

– вивчити призначення та сферу дії стандарту (0 ВСТУП, 0.1. Загальні положення, 1. Сфера застосування);

– ознайомитись із загальною побудовою змісту стандарту (з'ясувати кількість та найменування розділів);

– опрацювати всі розділи стандарту.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу дії стандарту (0 ВСТУП, 0.1. Загальні положення, 1. Сфера застосування);*
2. *Доповісти про загальну побудову змісту стандарту, кількість та найменування (спрямованість) розділів (складається із 10 розділів на 22 сторінках, спрямованість розділів, Додаток А)?*
3. *Які зобов'язання покладаються на керівництво установи з питань організації системи управління інформаційною безпекою (розділ 5, п. 5.1)?*
4. *Які вимоги встановлені стандартом щодо формування Політики інформаційної безпеки установи (розділ 5, п. 5.2)?*
5. *Які заходи передбачає оцінка ризиків інформаційної безпеки (розділ 6, п. 6.2.2)?*
6. *Які обов'язкові заходи повинні бути реалізовані в установі щодо документування процесів управління інформаційною безпекою (розділ 7, п. 7.5 за сукупністю вимог всього пункту)?*
7. *Як ви уявляєте організацію оцінювання результативності управління інформаційною безпекою в установі (за результатами аналізу*

положень розділу 9, за сукупністю положень всього розділу)?

8. *В ролі посадової особи служби захисту інформації установи прокоментуйте корисність інформації, наданої у Додатку А.*

Отже, міжнародний стандарт ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в установах, встановлює загальні вимоги до оцінки й обробки ризиків інформаційної безпеки з урахуванням потреб установи. Вимоги, які викладені в ISO/IEC 27001 є загальними та призначені для застосування всіма установами, незалежно від їхнього типу, розміру й характеру.

Міжнародний стандарт ISO/IEC 27002 "Інформаційні технології – Методи захисту – Звід практик щодо заходів інформаційної безпеки".

Цей міжнародний стандарт розроблено для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001 або як настанову для установ, які впроваджують загальноприйняті заходи інформаційної безпеки.

Стандарт призначено для використання його положень у розробленні настановчих документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їхнього середовища.

Інформаційної безпеки досягають впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури й програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та, за потреби, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілей організації. СУІБ, як це визначено в ISO/IEC 27001 та ISO/IEC 27002, надає цілісний, узгоджений розгляд ризиків інформаційної безпеки організації для того, щоб упровадити всебічний набір заходів інформаційної безпеки в межах загальних принципів зрозумілої системи управління.

Обсяг завдань щодо вивчення положень міжнародного стандарту ISO/IEC 27002:

– вивчити призначення та сферу дії стандарту (0 ВСТУП, 0.1. Загальні положення);

– ознайомитись із загальною побудовою змісту стандарту (з'ясувати кількість та найменування, спрямованість розділів);

– опрацювати всі розділи стандарту.

Контрольні питання та завдання:

1. *Доповісти про призначення та сферу застосування стандарту (0 ВСТУП, 0.1. Загальні положення, Розділ 1. Сфера застосування);*
2. *Доповісти про загальну побудову змісту стандарту, кількість та найменування (спрямованість) розділів (Розділ 4, п. 4.1, складається із 14 розділів на 66 сторінках, спрямованість розділів)?*
3. *Які вимоги встановлені стандартом щодо формування Політики інформаційної безпеки установи (розділ 5, п. 5.1.1)?*
4. *Які заходи передбачені стандартом щодо організації інформаційної безпеки (розділ 6, п. 6.2.1, 6.2.2)?*
5. *Які заходи безпеки повинні бути реалізовані у разі використання мобільного обладнання (розділ 6, п. 6.2.1)?*
6. *Які заходи безпеки повинні бути реалізовані у разі віддаленої роботи посадових осіб установи (розділ 6, п. 6.2.2)?*
7. *Які заходи безпеки повинні бути реалізовані з метою мінімізації ризиків, пов'язаних із "людським фактором" (розділ 7, п. п. 7.1.1, 7.1.2)?*
8. *Які заходи повинна містити політика використання криптографічних засобів для захисту інформації (розділ 10, п. 10.1.1, 10.1.2)?*
9. *Доповісти про положення стандарту, що стосуються організації фізичного захисту інфраструктури установи (розділ 11, п. 11.1.1);*
10. *В ролі посадової особи служби внутрішньої безпеки установи прокоментуйте корисність інформації, наданої у даному стандарті.*

Отже, положення міжнародного стандарту ISO/IEC 27002 оптимізують роботу фахівців підрозділів інформаційної безпеки установ щодо вибору заходів безпеки під час впровадження системи управління інформаційною безпекою (СУІБ) з метою їх включення до настановчих (організаційно-розпорядчих) документів з управління інформаційною безпекою, з подальшою їх практичною реалізацією в установах.

Міжнародний стандарт ISO/IEC 9798-1:2002 (9798-3:2002).

Розглянуті вище міжнародні стандарти групу стандартів ISO 27000 – СУІБ (ISO/IEC 27001 та ISO/IEC 27002) визначають загальні положення щодо організації та упровадження *системи управління інформаційною безпекою установи (далі – СУІБ).*

Окрім стандартизації загальних процесів, пов'язаних із СУІБ, існує ціла низка міжнародних стандартів (десятки найменувань), положення

яких стосуються різних аспектів в галузі інформаційних технологій, таких як: реалізація моделей автентифікації суб'єктів, реалізація протоколів керування ключами у разі використання КЗІ, реалізація криптографічних методів захисту інформації, що ґрунтуються на еліптичних кривих, встановлення критеріїв оцінки безпеки ІТ-технологій тощо.

На прикладі міжнародного стандарту ISO/IEC 9798-1:2002 "Інформаційні технології. Методи захисту. Автентифікація суб'єктів (Частина 1. Загальні положення)" доцільно вивчити загальну побудову та спрямованість змісту стандарту на реалізацію моделей автентифікації суб'єктів в ІС.

Обсяг завдань щодо роботи з положеннями міжнародного стандарту ISO/IEC 9798-1:2002 "Інформаційні технології. Методи захисту. Автентифікація суб'єктів (Частина 1. Загальні положення)":

– вивчити призначення, сферу дії стандарту та встановлену термінологію (Національний вступ, Розділ І. Сфера застосування, Розділ ІІІ);

– ознайомитись із загальною побудовою змісту стандарту (з'ясувати кількість та найменування, спрямованість розділів);

– опрацювати усі розділи стандарту.

Контрольні завдання:

1. *Доповісти про призначення та сферу застосування стандарту (Національний вступ, Розділ 1. Сфера застосування);*
2. *Доповісти про загальну побудову змісту стандарту, кількість та найменування (спрямованість) розділів (складається із 6 розділів на 6 сторінках, спрямованість розділів, Додатків А, В, С, D, зміст додатків)?*
3. *Наведіть визначення поняттям "асиметричний криптографічний метод", "асиметрична пара ключів", "асиметрична система підпису" "автентифікація суб'єкта", "взаємна автентифікація" (розділ 3, п. п. 3.3.1, 3.3.3, 3.3.4, 3.3.11, 3.3.14);*
4. *Поясніть суть реалізації автентифікації за моделлю, наведеної на рисунку 1 стор.5 стандарту (розділ 5);*
5. *Поясніть спрямованість змісту кожного із додатків А, В, С, D;*
6. *В ролі адміністратора безпеки ІС прокоментуйте корисність інформації, наданої у даному стандарті.*

Отже, міжнародний стандарт ISO/IEC 9798-1:2002 "Інформаційні технології. Методи захисту. Автентифікація суб'єктів (Частина 1. Загальні

положення)" визначає модель автентифікації, загальні вимоги та обмеження для механізмів автентифікації суб'єктів із використанням методів захисту. Положення стандарту є корисними для створення та упровадження захищених методів автентифікації користувачів ІС.

Положення міжнародного стандарту ***ISO/IEC 9798-3:2002 "Інформаційні технології. Методи захисту. Автентифікація суб'єктів" (Частина 3. Механізми з використання методу цифрового підпису)"*** доцільно розглянути курсантам самостійно під час самостійної роботи.

Отже, кожний із вивчених міжнародних стандартів адаптований у загальну систему нормативно-правового забезпечення ІБ держави, має своє призначення та місце у переліку головних НПА держави з метою досягнення максимального наближення до вимог та норм, які є загальноприйнятними для усіх країн-членів ЄС та НАТО, забезпечення участі України в загальноєвропейській та регіональній системах колективної безпеки, міжнародних проєктах економічної, політичної, екологічної, гуманітарної, миротворчої та інших видів діяльності під егідою ООН та ОБСЄ.

Інтеграція міжнародних стандартів та норм у національну систему нормативно-правового забезпечення ІБ України складає передумови успішного вирішення завдань, покладених на суб'єктів ІБ, як на міжнародній арені, так і всередині держави.

Саме про різноманіття та багатовекторність завдань, повноважень та зобов'язань суб'єктів ІБ держави мова піде у наступному підрозділі посібника.

1.6 Класифікація та повноваження суб'єктів забезпечення ІБ України

Як відомо зі змісту глави 1.1 для реалізації стратегії інформаційної безпеки та виконання завдань інформаційної безпеки держави створена система забезпечення інформаційної безпеки.

До складу системи забезпечення інформаційної безпеки держави належать:

– об'єкти забезпечення ІБ держави;

– ***суб'єкти забезпечення ІБ держави;***

– система нормативно-правового забезпечення її функціонування.

1.6.1 Загальна класифікація суб'єктів забезпечення ІБ України

Загальну класифікацію (перелік) ***суб'єктів забезпечення ІБ держави*** на підставі положень п.4 Закону України "Про інформацію" від 02 жовтня 1992 року № 2657-XII (зі змінами) [12] та положень Закону України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII [11] можна подати таким чином:

а) суб'єкти, які забезпечують формування, реалізацію державної політики у сфері ІБ, координацію, контроль за діяльністю суб'єктів ІБ:

Президент України;
Верховна Рада України;
Рада національної безпеки і оборони України;
Кабінет Міністрів України;

б) суб'єкти державного рівня, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення ІБ:

Міністерства, відомства, центральні органи виконавчої влади (в тому числі Міністерство закордонних справ, Державний комітет телебачення і радіомовлення України; Міністерство інформаційної політики України, Міністерство цифрової трансформації та інші;

спеціальні служби та міністерства України (СБУ, МВС, СЗР, **ДССЗЗІ;** ЗСУ, інші силові правоохоронні органи);

суди загальної юрисдикції;

прокуратура України;

місцеві державні адміністрації та органи місцевого самоврядування;

в) інші учасники інформаційних відносин в державі:

юридичні особи,

фізичні особи,

об'єднання громадян (за ознаками різного характеру).

Для діяльності всіх вищевказаних суб'єктів спільним є мета – *забезпечення інформаційного суверенітету та безпеки держави, забезпечення конституційних прав і свобод її громадян.*

Щодо досягнення цієї мети у положеннях п. 3 "Доктрини інформаційної безпеки України" (введено в дію указом Президента України від 25 лютого 2016 року № 47/2017) визначені такі ***загальні напрямки діяльності для усіх суб'єктів забезпечення ІБ держави:***

захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни,

розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

забезпечення вільного обігу інформації, крім випадків, передбачених законом;

розвиток та захист національної інформаційної інфраструктури;

збереження і примноження духовних, культурних і моральних цінностей Українського народу;

забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

зміцнення інформаційних зав’язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

розвиток системи стратегічних комунікацій України;

ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та в супутниковому мовленні за межами України.

Отже, положеннями чинних законодавчих та нормативно-правових актів визначені категорії суб'єктів забезпечення інформаційної безпеки держави та їх загальні напрямки діяльності.

Окрім загальних напрямків діяльності щодо забезпечення ІБ держави кожному суб'єкту визначені (відповідно до його місця в загальній класифікації) індивідуальні повноваження, права та обов'язки.

Послідовно розглянемо їх.

1.6.2 Повноваження суб'єктів державного рівня

Повноваження суб'єктів, які забезпечують формування, реалізацію державної політики у сфері ІБ, координацію, контроль за діяльністю суб'єктів системи ІБ держави.

У положеннях Конституції (Основного закону), Законів України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII, "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII кожному із суб'єктів забезпечення ІБ держави встановлені відповідні повноваження: [11, 19]

Президент України

як глава держави, гарант державного суверенітету додержання конституційних прав і свобод громадян, Верховний Головнокомандувач ЗС України і Глава РНБО України здійснює загальне керівництво та координацію усіх гілок влади щодо забезпечення НБ в інформаційній сфері; ухвалює нормативно-правові акти в цій сфері, визначає реальні та потенційні загрози для національної безпеки в інформаційній сфері, вживає необхідних заходів щодо її забезпечення.

До переліку його основних повноважень входять:

забезпечення державної незалежності, національної безпеки та територіальної цілісності;

здійснення зовнішньополітичної діяльності, представлення держави в міжнародних відносинах, укладання міжнародних договорів України;

очолення діяльності РНБО України;

визначення та затвердження основ політики національної безпеки України;

здійснення керівництва в інформаційній та інших сферах національної безпеки та оборони України, ухвалення відповідних Стратегій розвитку;

здійснення контролю за реалізацією заходів національної безпеки в межах своїх повноважень;

видання указів та розпоряджень у сфері ІБ, вимоги яких є обов'язковими для усіх інших суб'єктів забезпечення ІБ держави;

та інші повноваження, що визначені Конституцією.

Верховна Рада України

як вищий законодавчий орган держави, відповідно до положень Конституції України, визначає засади внутрішньої та зовнішньої політики (в тому числі і в інформаційній сфері), основи національної безпеки в інформаційній сфері, формує законодавчу базу в цій сфері, визначає загальну структуру та функції головних суб'єктів системи національної безпеки в інформаційній сфері.

Головними повноваженнями Верховної Ради у сфері ІБ держави є:

визначення засад внутрішньої та зовнішньої політики держави в інформаційній сфері;

здійснення законодавчого регулювання політики національної безпеки в інформаційній сфері (на законодавчому рівні закріплення прав, свобод, гарантій громадян в інформаційній сфері, встановлення цивільно-правової відповідальності осіб за не виконання законодавства у сфері інформаційних відносин, тощо);

створення правових засад функціонування системи забезпечення національної безпеки в інформаційній сфері;

затвердження бюджетних асигнувань для фінансування діяльності суб'єктів забезпечення ІБ України;

визначення порядку створення та повноважень РНБО України;

призначення на посади (або звільнення) за відповідними поданнями, передбаченими Конституцією України, на посади прем'єр-міністра України, голови СБУ, міністра Оборони України, міністра закордонних справ та інших посадових осіб, передбачених законом;

здійснення контролю за діяльністю Кабінету Міністрів України;

здійснення парламентського контролю за виконанням суб'єктами системи ІБ держави законодавства з питань національної безпеки в інформаційній сфері;

здійснення інших повноважень відповідно до Конституції України.

Рада національної безпеки і оборони України

як вищий координаційний орган з питань національної безпеки і оборони при Президенті України координує та контролює діяльність органів виконавчої влади в інформаційній та інших сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить пропозиції Президенту Украйни щодо уточнення Стратегії НБ держави. Рішення РНБО України вводяться в дію указами Президента України.

До головних повноважень Ради національної безпеки і оборони України у сфері ІБ держави належать:

внесення пропозицій Президентові України щодо реалізації засад внутрішньої та зовнішньої політики в інформаційній та інших сферах національної безпеки та оборони;

координація діяльності органів виконавчої влади щодо організації захисту громадян від негативних інформативних впливів та забезпеченню їхньої життєдіяльності в інформаційній сфері, охороні конституційних прав, свобод і законних інтересів, підтриманню громадського порядку в умовах воєнного та надзвичайного стану;

координація та здійснення контролю за діяльністю органів виконавчої влади в інформаційній та інших сферах національної безпеки та оборони у мирний час, умовах воєнного та надзвичайного стану та в разі виникнення кризових ситуацій, що загрожують національній безпеці держави;

залучення посадових осіб та фахівців інших суб'єктів системи ІБ держави до аналізу інформації щодо стану забезпечення національної безпеки в інформаційній та інших сферах національної безпеки та оборони;

ініціювання розроблення суб'єктами системи ІБ держави нормативно-правових актів та нормативних документів у сфері ІБ;

здійснення інших повноважень відповідно до Конституції України та чинного законодавства держави.

Кабінет Міністрів України

як вищий орган у системі органів виконавчої влади, підконтрольний і підзвітний Верховній Раді України, забезпечує державний (зокрема й інформаційний) суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод громадян, національної безпеки в інформаційній та інших сферах, громадського порядку та протидії злочинності.

Відповідно до положень ст. ст. 116, 117 Конституції України, ст. ст. 2, 19, 20 Закону України "Про Кабінет Міністрів України" від 27 лютого 2014 року № 794-VII головними повноваженнями Кабінету Міністрів України у сфері ІБ держави є:

забезпечення державного суверенітету та економічної самостійності України, здійснення внутрішньої та зовнішньої політики держави, виконання Конституції та законів України, актів Президента України, що стосуються безпеки в інформаційній сфері;

здійснення заходів щодо забезпечення обороноздатності і національної безпеки України, громадського порядку, боротьби зі злочинністю;

проведення державної політики у сфері інформатизації, сприяння становленню єдиного інформаційного простору на території України;

вжиття заходів щодо забезпечення прав і свобод людини та громадянина, створення сприятливих умов для вільного і всебічного розвитку особистості;

розроблення і виконання загальнодержавних програм економічного, науково-технічного, соціального, культурного розвитку України;

спрямування та координація роботи міністерств, інших органів виконавчої влади з локалізації та нейтралізації загроз національній безпеці та національним інтересам України в інформаційній сфері;

в межах своєї компетенції видання нормативно-правових актів у сфері ІБ, вимоги яких є обов'язковими для виконання іншими суб'єктами системи забезпечення ІБ держави;

в межах своїх повноважень здійснення контролю за реалізацією заходів з питань забезпечення національної безпеки в інформаційній сфері міністерствами та іншими органами виконавчої влади держави;

здійснення інших повноважень відповідно до Конституції України та чинного законодавства держави.

Вище розглянуті повноваження суб'єктів системи ІБ держави вищого рівня можуть бути змінені чи доповнені тільки на законодавчому рівні шляхом внесення правок та змін до змісту чинних законодавчих актів держави.

Повноваження суб'єктів державного рівня, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення ІБ.

Відповідно до класифікації суб'єктів системи забезпечення ІБ держави, розглянутої вище, до переліку суб'єктів цього рівня належить чимала кількість міністерств, відомств, центральних органи виконавчої влади, спеціальних служб, силових органів України тощо.

Розглянемо повноваження головних із переліку цих суб'єктів.

Міністерство закордонних справ України (далі – МЗС України)

виконує покладені на нього повноваження у сфері ЗІБ, передбачені "Положенням про Міністерство закордонних справ України", введеного в дію постановою КМ України від 30 березня 2016 р. № 281.

Основними повноваженнями МЗС України в сфері ІБ є:

формування та реалізація державної політики у сфері зовнішніх зносин України;

забезпечення провадження зовнішньополітичної діяльності держави;

забезпечення проведення зовнішньополітичного курсу України, спрямованого на розвиток політичних, економічних, гуманітарних,

правових, наукових та інших зав’язків з іноземними державами, міжнародними організаціями, та здійснення аналізу відповідних тенденцій у цих сферах;

забезпечення дипломатичними засобами й методами захисту суверенітету, міжнародної безпеки, територіальної цілісності та непорушності кордонів України, її національних інтересів, зокрема в інформаційній сфері;

сприяння всебічній інтеграції України у світовий інформаційний простір, піднесенню її міжнародного авторитету, формуванню позитивного іміджу держави як надійного та передбачуваного партнера;

забезпечення розвитку зав’язків із закордонними українцями та їхніми громадськими об'єднаннями, координація заходів, що здійснюються органами виконавчої влади з метою розвитку таких зав’язків;

координація діяльності державних органів щодо забезпечення реалізації єдиного зовнішньополітичного курсу України;

участь у формуванні та реалізації державної політики, спрямованої на інтеграцію України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору;

забезпечення національних інтересів і міжнародної безпеки України шляхом підтримання мирного та взаємовигідного співробітництва з іноземними державами і міжнародними організаціями за загальновизнаними принципами та нормами міжнародного права;

забезпечення функціонування власної мережі телекомунікаційної і кур'єрської служби та організація доставки дипломатичної пошти;

забезпечення координації діяльності, що здійснюється державними органами у сфері зовнішніх зносин, сприяння державним органам у частині здійснення ними зовнішніх зносин, надання їм відповідної методичної, консультаційної та інформаційної допомоги, дотримання міжнародних зобов'язань України;

спрямовування, координування та контроль у встановленому порядку діяльності відповідних структурних підрозділів місцевих державних адміністрацій у сфері зовнішніх зносин;

та інші.

МЗС України здійснює свої повноваження безпосередньо та через представництва МЗС України на території держави, закордонні дипломатичні установи України, підприємства, установи й організації, що належать до сфери його управління.

Міністерство культури та інформаційної політики (далі – МКІП)

є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України у сфері

забезпечення інформаційного суверенітету України, поширенню суспільно важливої інформації в державі та за її межами, забезпечення функціонування державних інформаційних ресурсів.

Головними напрямками діяльності МКІП є:

забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в державі та за її межами, а також забезпечення функціонування державних інформаційних ресурсів;

забезпечення здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації.

Відповідно до головних напрямків діяльності на МКІП покладені такі повноваження:

упорядкування нормативно-правового забезпечення ІБ: розробка та погодження проєктів законів України та інших НПА з питань, що входять до його компетенції;

підготовка відповідних пропозицій та зауважень до прийнятих ВР України законів, що надійшли на підпис Президенту України;

участь у формуванні державної інформаційної політики;

впровадження заходів щодо захисту прав громадян на вільний збір, зберігання, використання та поширення інформації, в т.ч. на тимчасово окупованих територіях та районах ведення бойових дій;

координація діяльності органів виконавчої влади та взаємодія з органами місцевого самоврядування з питань, віднесених до компетенції МКІП;

розробка разом з МЗС та МОН планів заходів та програмних документів щодо позитивного позиціювання України у світі;

забезпечення проведення фестивалів, виставок;

утворення спеціалізованих експертних рад МКІП;

здійснення інших повноважень, визначених чинним законодавством.

Міністерство цифрової трансформації (далі – Мінцифри)

Міністерство цифрової трансформації України – центральний орган виконавчої влади, який відповідає за формування та реалізацію державної політики у сфері цифровізації, відкритих даних, національних електронних інформаційних ресурсів, інтероперабельності – взаємодії мережевих систем на базі уніфікованих інтерфейсів або протоколів, впровадження електронних послуг та розвиток цифрової грамотності громадян. Міністерство було створене у вересні 2019 року.

Основними повноваженнями Мінцифри в сфері ІБ є:

формування та реалізація державної політики у сфері цифровізації, цифрової економіки, цифрових інновацій, електронного урядування та електронної демократії, розвитку інформаційного суспільства;

формування та реалізація державної політики у сфері розвитку цифрових навичок та цифрових прав громадян;

формування та реалізація державної політики у сфері відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу;

формування та реалізація державної політики у сфері надання електронних та адміністративних послуг;

формування та реалізація державної політики у сфері електронних довірчих послуг;

формування та реалізація державної політики у сфері розвитку ІТ-індустрії;

виконання функцій ***центрального засвідчувального органу*** шляхом створення умов для функціонування суб'єктів правових відносин у сфері електронних довірчих послуг.

Функції та повноваження ***центрального засвідчувального органу*** визначено у Статті 7 Закону України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII, (зі змінами), відповідно до якої Мінцифра: [59]

здійснює визначені законом повноваження у сферах електронних довірчих послуг та електронної ідентифікації;

надає адміністративну послугу шляхом внесення юридичних осіб та фізичних осіб-підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку;

погоджує розроблені надавачами електронних довірчих послуг порядки синхронізації часу зі Всесвітнім координованим часом (UTC);

погоджує плани припинення діяльності кваліфікованих надавачів електронних довірчих послуг;

приймає та зберігає документовану інформацію, сформовані сертифікати (зокрема посилені, кваліфіковані) відкритих ключів, реєстри чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності кваліфікованого надавача електронних довірчих послуг;

розглядає пропозиції (зауваження) суб'єктів відносин у сфері електронних довірчих послуг щодо удосконалення державного регулювання сфери електронних довірчих послуг;

надає суб'єктам відносин у сфері електронних довірчих послуг консультації з питань, пов'язаних з наданням електронних довірчих послуг;

інформує відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги" про обставини, які перешкоджають діяльності центрального засвідчувального органу;

проводить оцінку стану розвитку сфери електронних довірчих послуг за результатами проведення аналізу інформації про діяльність постачальників електронних довірчих послуг та засвідчувального центру;

забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг;

здійснює інші повноваження у сферах електронних довірчих послуг та електронної ідентифікації, визначені законом.

Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу – державним підприємством, яке належить до сфери управління Мінцифри (державним підприємством “ДІЯ”).

Служба безпеки України (далі – СБУ)

є одним із провідних суб’єктів реалізації державної політики України у інформаційній сфері, на який покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного, оборонного потенціалу держави, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спецслужб, забезпечення охорони державної таємниці.

До напрямків діяльності СБУ також належать запобігання, припинення та розкриття злочинів проти миру й безпеки людства, протидія тероризму, корупції, організованій злочинній діяльності у сфері управління та економіки, комп’ютерній злочинності, намаганням маніпулювати суспільною свідомістю та іншими чинниками, які безпосередньо загрожують національній безпеці.

Основними повноваженнями СБУ в сфері ІБ є:

постійний моніторинг впливу на національну безпеку процесів, що відбуваються в першу *чергу в інформаційній*, політичній, соціальній, економічній, науково-технологічній, воєнній сферах; прогнозування змін, що відбуваються в них; виявлення потенційних загроз національній безпеці;

систематичне спостереження за станом і проявами міжнародного та інших видів тероризму (*у т.ч. – кібертероризму*);

прогнозування, виявлення, оцінка можливих загроз, причин і умов їх виникнення та наслідків прояву;

комплексне інформаційно-аналітичне забезпечення діяльності вищих органів влади та інших суб'єктів забезпечення нацбезпеки держави в інформаційній сфері;

розроблення науково обґрунтованих пропозицій щодо ухвалення управлінських рішень з метою захисту національних інтересів;

запобігання й нейтралізація впливу загроз і дестабілізуючих чинників на національну безпеку та національні інтереси в інформаційній сфері;

проведення планових та оперативних заходів з компетентними структурами іноземних держав у рамках міжнародних організацій та договорів у галузі безпеки;

контроль стану охорони державної таємниці в усіх органах державної влади, органах місцевого самоврядування, на підприємствах, в установах та організаціях держави, діяльність яких пов'язана із державною таємницею;

здійснення інших повноважень, визначених чинним законодавством.

Міністерство внутрішніх справ України (далі – МВС України)

є одним із суб'єктів реалізації державної політики України в інформаційній сфері, який із використанням форм і методів, передбачених законами України "Про національну поліцію", "Про оперативно-розшукову діяльність", "Про боротьбу з корупцією" та іншими НПА у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки здійснюють свої повноваження щодо нейтралізації загроз національній безпеці України в інформаційній сфері.

Відповідно до п. 3 "Положення про Міністерство внутрішніх справ України", введеного в дію постановою КМУ від 28 жовтня 2015 року № 878, основними повноваженнями МВС України в сфері ІБ є:

забезпечення формування державної політики у сфері охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, забезпечення публічної безпеки і порядку, а також надання поліцейських послуг;

організація і координація діяльності органів внутрішніх справ щодо захисту прав і свобод громадян, інтересів суспільства і держави, охороні громадського порядку і безпеки в інформаційній сфері;

запобігання злочинам в інформаційній сфері, їх припинення, розкриття і розслідування, розшуку осіб, які вчинили злочини, вжиття заходів щодо усунення причин та умов, що сприяють вчиненню правопорушень;

організація охорони та оборони внутрішніми військами особливо важливих державних об'єктів, у т.ч. об'єктів критичної інфраструктури держави;

підготовка органів внутрішніх справ і структурних підрозділів для інтеграції України до ЄС;

здійснення інших повноважень, визначених чинними НПА.

Подібні повноваження у сфері забезпечення ІБ держави відповідними НПА визначені й іншим суб'єктам.

Отже, кожний суб'єкт забезпечення ІБ у межах своїх повноважень, встановлених відповідними законодавчими та нормативно-правовими актами України, на своєму ієрархічному рівні є провідником державної політики національної безпеки в інформаційній сфері. Від якості, повноти, узгодженості виконання повноважень, функцій та завдань усіх суб'єктів залежить загальний результат забезпечення інформаційної безпеки держави в цілому.

1.6.3 Повноваження та завдання Державної служби спеціального зв'язку та захисту інформації України щодо забезпечення ІБ держави

До переліку суб'єктів забезпечення ІБ держави належить ***Державна службу спеціального зв'язку та захисту інформації України,*** *до якої мають безпосереднє відношення здобувачі вищої освіти ІСЗЗІ НТУУ "КПІ" ім. Ігоря Сікорського.* Саме ці обставини зумовлюють необхідність уважного вивчення повноважень та функцій, які покладено в державі на нашу службу. Після випуску з інституту та призначення на первинні посади у відповідні структурні підрозділи служби, певні із цих функцій стануть основним змістом ваших повсякденних функціональних обов'язків.

Відповідно до положень ст. ст. 2, 3 Закону України ***"Про державну службу спеціального зв'язку та захисту інформації" від 23 лютого 2006 року № 3475-IV*** Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України. [27]

Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку ***державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону.***

Основними повноваженнями Державної служби спеціального зв'язку та захисту інформації України є:

а) формування та реалізація державної політики у сферах: *(повноваження тільки ДССЗЗІ)*:

криптографічного та технічного захисту інформації;

кіберзахисту;

поштового зв'язку спеціального призначення;

урядового фельд'єгерського зв'язку;

захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – інформаційно-комунікаційні системи) і на об'єктах інформаційної діяльності.

б) формування та реалізація державної політики у сферах використання державних інформаційних ресурсів (*повноваження тільки ДССЗЗІ)*:

в частині захисту інформації;

протидії технічним розвідкам;

функціонування, безпеки та розвитку державної системи урядового зв'язку;

функціонування, безпеки та розвитку Національної системи конфіденційного зв'язку;

активної протидії агресії у кіберпросторі.

в) участь у формуванні та реалізації державної політики *(разом із іншими суб'єктами забезпечення ІБ)* у сферах:

електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування);

електронної ідентифікації (з використанням електронних довірчих послуг, захисту критичної інформаційної інфраструктури);

електронних довірчих послуг;

захисту критичної інформаційної інфраструктури (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, захисту критичної інформаційної інфраструктури, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг, захисту критичної інформаційної інфраструктури);

забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

г) реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах, в тому числі:

визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об’єктів критичної інфраструктури, ведення переліку об’єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі;

створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі;

виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту.

Державна служба спеціального зв’язку та захисту інформації України має таку загальну структуру:

центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку, захисту інформації (далі – *Адміністрація Держспецзв’язку України*);

територіальні органи центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку та захисту інформації;

територіальні підрозділи ДССЗЗІ;

Головне управління та підрозділи урядового фельд’єгерського зв’язку;

навчальні, охорони здоров’я, санаторно-курортні та інші заклади, науково-дослідні, науково-виробничі та інші установи і організації.

Кожному органу, підрозділу, закладу визначені повноваження та функції відповідно до його статусу та призначення.

Докладно розглянемо повноваження, що покладені на Адміністрацію Держспецзв’язку, територіальні органи Адміністрації Держспецзв’язку та територіальні підрозділи ДССЗЗІ.

<u>Адміністрація Держспецзв’язку</u>

є центральним органом виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України через віце-прем’єр-міністра України з інновацій, розвитку освіти, науки та технологій – міністра цифрової трансформації і який забезпечує

формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, кіберзахисту, активної протидії агресії у кіберпросторі.

Вона є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації; центральним органом виконавчої влади, який забезпечує здійснення Держспецзв'язку повноважень уповноваженого органу в сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, передбачених Законом України "Про критичну інфраструктуру України".

Відповідно до ***"Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України", затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 р. № 411*** на Адміністрацію Держспецзв'язку покладені наступні повноваження: [28]

1) забезпечення формування та реалізація:

державної політики у сферах криптографічного і технічного захисту інформації, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – інформаційно-комунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку Національної телекомунікаційної мережі, державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; у сферах захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у таких сферах;

державної політики у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування;

2) участь у формуванні та реалізації:

державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), захисту критичної інформаційної інфраструктури, електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг);

3) реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснення державного контролю у зазначених сферах.

Адміністрація Держспецзв’язку відповідно до покладених на неї завдань:

1) узагальнює практику застосування законодавства з питань, що належать до її компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України і Кабінету Міністрів України та в установленому порядку вносить їх на розгляд Кабінету Міністрів України;

2) розробляє проєкти законів та інших нормативно-правових актів з питань, що належать до її компетенції;

3) погоджує проєкти законів, інших актів законодавства, які надходять на погодження від інших центральних органів виконавчої влади, готує в межах повноважень, передбачених законом, висновки і пропозиції до проєктів законів, інших актів законодавства, які подаються на розгляд Кабінету Міністрів України, та проєктів законів, внесених на розгляд Верховної Ради України іншими суб’єктами права законодавчої ініціативи, нормативно-правових актів Верховної Ради Автономної Республіки Крим;

4) готує в межах повноважень, передбачених законом, зауваження і пропозиції до прийнятих Верховною Радою України законів, що надійшли на підпис Президентові України;

5) здійснює державне регулювання у сфері поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку;

6) забезпечує нормативно-правове регулювання у сферах криптографічного і технічного захисту інформації, організації спеціального зв’язку, урядового фельд’єгерського зв’язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у кіберпросторі, в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, протидії технічним розвідкам, кіберзахисту об’єктів критичної інформаційної інфраструктури;

7) здійснює технічне регулювання у сферах криптографічного і технічного захисту інформації, кіберзахисту об’єктів критичної інфраструктури, протидії технічним розвідкам, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, організацію, координацію та проведення робіт з підтвердження відповідності, розроблення в установленому порядку технічних регламентів; здійснює державний ринковий нагляд у межах сфери своєї відповідальності;

8) здійснює методичне керівництво та координацію діяльності державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності у сферах криптографічного і технічного захисту інформації, протидії технічним розвідкам, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-комунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах;

9) організовує забезпечення урядовим фельд'єгерським зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів місцевого самоврядування, органів військового управління та інших юридичних осіб відповідно до законодавства;

10) організовує забезпечення урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного стану і в особливий період;

11) організовує забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку, її готовності до роботи в особливий період і в разі виникнення надзвичайної ситуації;

12) здійснює заходи щодо організації та забезпечення безпеки і функціонування урядового зв'язку із закордонними дипломатичними установами України;

13) організовує та забезпечує укладення договорів оренди приміщень, майна, а також ресурсів електронних комунікаційних мереж для задоволення потреб Національної телекомунікаційної мережі, державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

14) контролює виконання вимог законодавства у сфері захисту інформації в приміщеннях абонентів урядового зв'язку;

15) вирішує в межах повноважень, передбачених законом, питання забезпечення зв'язку для потреб державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, відповідних державних органів згідно із законодавством;

забезпечує здійснення Держспецзв'язку передбачених Законом України "Про критичну інфраструктуру України" повноважень ***уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану***, а також протягом 12 місяців після його припинення чи скасування;

16) установлює порядок:

створення та розвитку систем спеціального зв’язку;

розроблення, виготовлення та постачання ключових документів до засобів криптографічного захисту інформації, що містить державну таємницю, службову інформацію та публічну інформацію з обмеженим доступом;

ведення та керування реєстром інформаційно-комунікаційних систем державних органів, а також підприємств, установ і організацій, що належать до сфери їх управління, ведення Національного реєстру електронних інформаційних ресурсів органів державної влади;

надання послуг Національної телекомунікаційної мережі на умовах, визначених Правилами надання послуг, які надаються з використанням Національної телекомунікаційної мережі;

17) установлює порядок організації та проведення державної експертизи у сфері криптографічного і технічного захисту інформації, проводить державну експертизу та експертні дослідження у сфері криптографічного захисту інформації, визначає криптографічні алгоритми як рекомендовані, допускає до експлуатації засоби криптографічного захисту інформації, засоби, комплекси та системи спеціального зв’язку, надає та/або реєструє експертні висновки за результатами державної експертизи у сфері криптографічного та технічного захисту інформації, свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, засобів, комплексів та систем спеціального зв’язку, декларації та атестати відповідності комплексних систем захисту інформації;

18) установлює порядок створення та допуску до експлуатації, допускає до експлуатації засоби криптографічного захисту службової інформації та інформації, що становить державну таємницю, засоби, комплекси та системи спеціального зв’язку, визначає криптографічні алгоритми для застосування у засобах криптографічного захисту інформації;

19) установлює порядок надання висновків та погоджень міжнародних передач криптосистем, засобів криптографічного і технічного захисту інформації, зокрема тих, що є складовими частинами озброєння, військової та спеціальної техніки, надає такі висновки й погодження;

20) установлює порядок здійснення державного контролю і здійснює державний контроль:

за станом криптографічного і технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від форми власності, зокрема в закордонних дипломатичних установах України, національних контингентах за кордоном, місцях постійного і

тимчасового перебування Президента України, Голови Верховної Ради України та Прем’єр-міністра України, а також під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов’язковість яких надана Верховною Радою України;

за дотриманням вимог законодавства у сфері електронних довірчих послуг;

за станом протидії технічним розвідкам у державних органах, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від їхнього підпорядкування та форми власності, які мають у своєму володінні, користуванні чи розпорядженні зразки озброєння, військової та спеціальної техніки, об’єкти оборонно-промислового комплексу, військові об’єкти та інші об’єкти, призначені для застосування в інтересах оборони і безпеки держави;

за додержанням вимог безпеки під час розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, проведення тематичних досліджень, експертизи, вивезення та знищення криптографічних систем і засобів криптографічного захисту інформації та обладнання спеціального зв’язку, що мають гриф обмеження доступу;

за станом захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури;

21) організовує впровадження комплексних систем захисту інформації на об’єктах інформаційної діяльності та в інформаційно-комунікаційних системах закордонних дипломатичних установ України за рахунок коштів, передбачених у законі про Державний бюджет України на функціонування та утримання таких установ;

22) установлює порядок та вимоги технічного захисту інформації на об’єктах інформаційної діяльності, створення та атестації комплексів технічного захисту інформації, реєструє акти атестації комплексів технічного захисту інформації;

23) визначає переліки засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;

24) установлює дозвільний порядок, видає, переоформлює, зупиняє (поновлює) дію, анулює дозволи (копії і дублікати дозволів) на проведення робіт із технічного захисту інформації для власних потреб;

25) організовує та координує роботи з проведення сертифікації засобів криптографічного і технічного захисту інформації разом із центральним органом виконавчої влади з питань технічного регулювання;

26) погоджує регламенти роботи центрального засвідчувального органу, засвідчувального центру, кваліфікованих надавачів електронних довірчих послуг, а також надавачів електронних довірчих послуг та юридичних осіб, фізичних осіб-підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги;

27) встановлює вимоги щодо безпеки та захисту інформації для кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації;

28) здійснює повноваження органу ліцензування у сфері криптографічного і технічного захисту інформації;

29) організовує забезпечення функціонування, безпеки та розвитку Національної системи конфіденційного зв'язку;

30) розробляє критерії і порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційно-комунікаційних системах, організовує оцінку стану захищеності державних інформаційних ресурсів;

31) розробляє та затверджує єдині технічні вимоги щодо захисту Єдиного веб-порталу державних органів, контролює додержання цих вимог;

32) погоджує проєкти (завдання) створення та розвитку інформаційно-комунікаційних систем, систем спеціального зв'язку, систем електронного документообігу (в частині захисту інформації), в яких оброблятимуться державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом, програмно-технічних комплексів надавачів електронних довірчих послуг, засвідчувального центру та центрального засвідчувального органу (в частині захисту інформації), організовує проведення їх експертної оцінки;

33) розробляє і супроводжує моделі технічних розвідок шляхом збору та аналізу інформації про наявні системи й засоби технічних розвідок, розробляє тактики та методи їх застосування, а також перспективи розвитку, надає державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам і організаціям рекомендації щодо забезпечення протидії технічним розвідкам, проведення оцінки загроз і вжиття відповідних заходів для захисту інформації;

34) погоджує та здійснює контроль за виконанням технічних завдань на проєктування, будівництво і реконструкцію особливо важливих об'єктів і на розроблення зразків військової та спеціальної техніки в частині протидії технічним розвідкам;

35) подає Президентові України, Голові Верховної Ради України і Прем'єр-міністрові України за результатами державного контролю аналітичні матеріали щодо стану криптографічного і технічного захисту інформації, протидії технічним розвідкам у державі, розробляє рекомендації щодо його посилення;

36) бере участь у погодженні питань розміщення на території України дипломатичних представництв і консульських установ іноземних держав;

37) погоджує в порядку, встановленому законодавством, призначення керівників органів спеціального зв'язку, підрозділів з питань зв'язку, інформатизації та захисту інформації державних органів, Національного банку та Офісу Генерального прокурора;

38) виконує функції радіочастотного органу спеціального користувача радіочастотного спектра України;

39) установлює:

технічні вимоги до електронних комунікаційних мереж, систем і комплексів, засобів та об'єктів спеціального зв'язку;

порядок і забезпечує проведення експертизи інфраструктури електронних комунікацій проєктів будівництва, реконструкції та модернізації електронних комунікаційних мереж, споруд і засобів спеціального зв'язку;

40) здійснює управління електронними комунікаційними мережами та відповідає за забезпечення їх сталості в умовах надзвичайного та воєнного стану;

41) забезпечує розвиток у сферах криптографічного і технічного захисту інформації, кіберзахисту;

42) проводить відповідно до законодавства заходи щодо реалізації науково-технічної політики, організації наукового, науково-технічного забезпечення функціонування і розвитку сфер спеціального зв'язку та захисту інформації, кіберзахисту;

43) розробляє та організовує виконання державних цільових, наукових і науково-технічних програм за напрямами діяльності Держспецзв'язку;

44) вживає заходів для здійснення галузевої співпраці з іншими державами;

45) бере участь у підготовці міжнародних договорів України з питань, що належать до повноважень Держспецзв'язку, готує пропозиції щодо укладення, денонсації таких договорів і забезпечення їх виконання;

46) забезпечує в межах повноважень, передбачених законом, формування та реалізацію інноваційної та інвестиційної політики;

47) бере участь у реалізації державного замовлення на виконання робіт і поставок продукції для державних потреб, сприяння залученню інвестицій, новітніх технологій у сферах спеціального зв'язку та захисту інформації, кіберзахисту;

48) здійснює контроль якості та приймання продукції, інших товарів військового призначення, які виготовляються (модернізуються) на замовлення Держспецзв'язку;

49) бере участь у виконанні завдань з територіальної оборони, а також у заходах, спрямованих на підтримання правового режиму воєнного та надзвичайного стану відповідно до закону;

50) бере участь в межах повноважень, передбачених законом, у стратегічному плануванні застосування Збройних Сил, інших військових формувань, утворених відповідно до закону, і правоохоронних органів для оборони держави;

51) визначає потреби Держспецзв'язку у військовому майні на особливий період;

52) організовує забезпечення підрозділів Держспецзв'язку озброєнням, технікою, а також майном та ресурсами, необхідними для виконання покладених на Держспецзв'язку завдань;

53) визначає порядок придбання, перевезення та носіння вогнепальної зброї, боєприпасів до неї, інших предметів і матеріалів, на які поширюється дозвільна система, військовослужбовцями Держспецзв'язку;

54) установлює порядок організації служби з охорони об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації та вживає заходів для забезпечення їх збереження;

56) організовує вартову та внутрішню служби в Держспецзв'язку і встановлює особливості їх організації;

57) визначає порядок чергування особового складу Держспецзв'язку, а також несення ним служби (виконання роботи) у підземних спорудах зв'язку та вахтовим методом у зоні відчуження;

58) проводить відомчу реєстрацію, веде облік та організовує проведення обов'язкового технічного контролю транспортних засобів Держспецзв'язку;

59) організовує та здійснює разом з МОН науково-методичне управління підготовкою кадрів у сфері криптографічного і технічного захисту інформації, електронних комунікацій, радіотехнологій та користування радіочастотним ресурсом України;

60) організовує проведення професійно-психологічного відбору кандидатів на службу до Держспецзв'язку, психологічного забезпечення службової діяльності та встановлює порядок їх здійснення;

61) виступає державним замовником на підготовку, перепідготовку та підвищення кваліфікації особового складу Держспецзв'язку, в тому числі навчання операторів безпілотних систем (безпілотних авіаційних комплексів, безпілотних літальних апаратів, безпілотних наземних (роботизованих) комплексів, безпілотних водних (плаваючих) комплексів) із числа особового складу Держспецзв'язку та працівників інших державних органів;

62) установлює порядок здійснення добору кадрів у Держспецзв'язку, формування кадрового резерву, організовує роботу з підготовки, перепідготовки та підвищення кваліфікації особового складу Держспецзв'язку;

63) здійснює в межах повноважень, передбачених законом, функції з управління об’єктами державної власності, що належать до сфери управління Адміністрації Держспецзв’язку;

64) проводить планові та позапланові перевірки:

стану криптографічного і технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України, національних контингентах за кордоном, під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов’язковість яких надана Верховною Радою України, без одержання доступу до інформації (в місцях постійного та тимчасового перебування осіб, щодо яких здійснюється державна охорона, зазначені перевірки проводяться за погодженням з Управлінням державної охорони);

додержання ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного і технічного захисту інформації на підприємствах, в установах і організаціях, а також умов проведення робіт з технічного захисту інформації для власних потреб в державних органах, органах місцевого самоврядування, органах управління Збройних Сил та інших військових формувань, утворених відповідно до закону, правоохоронних органах;

кваліфікованих надавачів електронних довірчих послуг, їхніх відокремлених пунктів реєстрації, засвідчувального центру, центрального засвідчувального органу щодо дотримання вимог законодавства у сфері електронних довірчих послуг;

стану протидії технічним розвідкам в державних органах, військових формуваннях, утворених відповідно до закону, на підприємствах, в установах і організаціях незалежно від їхнього підпорядкування та форми власності, які мають у своєму володінні, користуванні чи розпорядженні зразки озброєння, військової та спеціальної техніки, об’єкти оборонно-промислового комплексу, військові об’єкти та інші об’єкти, призначені для застосування в інтересах оборони і безпеки держави;

65) зупиняє дію або скасовує в установленому порядку:

експертні висновки, видані за результатами державної експертизи у сфері технічного та криптографічного захисту інформації;

свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, криптографічних алгоритмів, засобів, комплексів та систем спеціального зв’язку, які призначені для захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, і криптографічних алгоритмів;

декларації та атестати відповідності комплексних систем захисту інформації в інформаційно-комунікаційних системах та акти атестації комплексів технічного захисту інформації на об’єктах інформаційної діяльності у разі ненадання допуску (доступу) або створення перешкод для такого допуску (доступу) уповноваженим посадовим особам Держспецзв’язку до проведення заходів державного контролю за станом технічного захисту інформації або за наявності порушень у сфері захисту інформації, яка обробляється в інформаційно-комунікаційних системах, якщо це створює реальну загрозу або передумови до порушення конфіденційності та/або цілісності та доступності інформації;

66) порушує в установленому порядку питання про:

припинення обробки інформації на об’єктах інформаційної діяльності або проведення інформаційної діяльності з використанням інформаційно-комунікаційних систем в державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до закону, на підприємствах, в установах і організаціях незалежно від форми власності, що проводиться з порушенням вимог законодавства у сфері захисту інформації, вимога щодо захисту якої встановлена законом, криптографічного та/або технічного захисту інформації; зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов’язаної з державною таємницею, у разі виявлення порушень у сфері криптографічного та/або технічного захисту інформації;

зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов’язаної з державною таємницею, у разі виявлення порушень у сфері криптографічного і технічного захисту інформації;

проведення службових розслідувань щодо з’ясування причин та умов виникнення порушень, виявлених за результатами державного контролю, здійснення якого покладено на Держспецзв’язку;

67) проводить експертні та тематичні дослідження у сфері криптографічного захисту інформації, зокрема на договірних засадах;

68) здійснює міжнародне співробітництво, розробляє пропозиції щодо укладення відповідних міжнародних договорів України, взаємодіє відповідно до міжнародних договорів України з міжнародними організаціями з питань, що належать до повноважень Держспецзв’язку;

69) забезпечує провадження господарської діяльності у порядку, передбаченому законодавством;

70) є замовником закупівлі товарів, робіт і послуг у сфері публічних закупівель, державним замовником у сфері оборони із закупівлі безпілотних систем (безпілотних авіаційних комплексів, безпілотних літальних апаратів, безпілотних наземних (роботизованих) комплексів, безпілотних водних (плаваючих) комплексів), засобів активної (радіоелектронної боротьби) та пасивної протидії технічним розвідкам, зокрема щодо їх виробництва, експлуатації, ремонту, та уповноважує

територіальні органи Адміністрації Держспецзв’язку, територіальні підрозділи, Головне управління та підрозділи урядового фельд’єгерського зв’язку, заклади, установи та організації, які входять до структури Держспецзв’язку, підприємства, установи, організації, що належать до сфери управління Адміністрації Держспецзв’язку, як служби державного замовника на здійснення закупівель та укладення державних контрактів (договорів) на закупівлю товарів, робіт і послуг оборонного призначення та інших товарів, робіт і послуг для гарантованого забезпечення потреб у сфері безпеки і оборони;

71) забезпечує в межах повноважень, передбачених законом, проведення заходів з охорони праці та пожежної безпеки в Держспецзв’язку;

72) провадить в установленому порядку видавничу діяльність;

73) висвітлює свою діяльність в засобах масової інформації і на веб-сайті Держспецзв’язку;

75) утворює військово-лікарську комісію Держспецзв’язку для проведення військово-лікарської експертизи і медичного огляду та встановлює порядок її діяльності;

76) координує діяльність суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

77) здійснює заходи із створення та забезпечення функціонування Національної телекомунікаційної мережі;

78) забезпечує впровадження організаційно-технічної моделі кіберзахисту;

79) забезпечує впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, їх атестації (переатестації);

80) координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

81) забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

82) визначає перелік послуг Національної телекомунікаційної мережі;

83) організовує акредитацію з безпеки комунікаційно-інформаційних систем (інформаційно-комунікаційних систем), де обробляється інформація НАТО з обмеженим доступом;

84) встановлює порядок акредитації з безпеки комунікаційно-інформаційних систем (інформаційно-комунікаційних систем), де обробляється інформація НАТО з обмеженим доступом;

85) надає консультації, розробляє вимоги і рекомендації з безпеки комунікаційно-інформаційних систем (інформаційно-комунікаційних систем), де обробляється інформація НАТО з обмеженим доступом;

86) проводить перевірку впроваджених заходів з безпеки комунікаційно-інформаційних систем (інформаційно-комунікаційних систем), де обробляється інформація НАТО з обмеженим доступом, щодо їх відповідності вимогам законодавства та надання рекомендацій стосовно коригувальних заходів;

87) погоджує застосування засобів криптографічного захисту інформації та апаратних засобів для передачі інформації НАТО з обмеженим доступом;

88) здійснює контроль за дотриманням держателями, адміністраторами, технічними адміністраторами публічних електронних реєстрів, держателем та технічним адміністратором системи електронної взаємодії електронних ресурсів, публічними реєстраторами та створювачами реєстрової інформації законодавства про захист інформації в інформаційно-комунікаційних системах та приймає обов'язкові до виконання рішення, передбачені законом;

89) бере участь у розробленні й забезпеченні виконання державних цільових програм з розвитку публічних електронних реєстрів у частині здійснення контролю за дотриманням законодавства про захист інформації в інформаційно-комунікаційних системах;

90) організовує роботу з підготовки та підвищення кваліфікації представників держателів, адміністраторів і технічних адміністраторів публічних електронних реєстрів, держателя та адміністратора системи електронної взаємодії електронних ресурсів з питань дотримання законодавства про захист інформації в інформаційно-комунікаційних системах;

91) забезпечує створення, функціонування та розвиток Національного центру резервування державних інформаційних ресурсів;

92) визначає вимоги до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури, ведення переліку об'єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

93) у межах своїх повноважень здійснює планування відповідних заходів із захисту критичної інфраструктури;

94) бере участь у розробленні плану взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури;

95) формує та веде національний перелік об'єктів критичної інформаційної інфраструктури;

96) здійснює управління Національною телекомунікаційною мережею як об'єктом державної власності;

97) створює та забезпечує функціонування системи активної протидії агресії у кіберпросторі;

98) створює та забезпечує функціонування Центру активної протидії агресії у кіберпросторі;

здійснює інші повноваження, визначені законом.

<u>Територіальні органи Адміністрації Держспецзв'язку</u>

входять до загальної структури ДССЗЗІ України, підпорядковуються Адміністрації Держспецзв'язку і забезпечують виконання покладених на Держспецзв'язку завдань на території Автономної Республіки Крим, областей, міст Києва та Севастополя, а у випадку, коли він утворений як міжрегіональний територіальний орган, – на території декількох адміністративно-територіальних одиниць, на які поширюються його повноваження (далі – регіон).

Відповідно до "Положення про територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України" введеного в дію наказом Адміністрації Держспецзв'язку України від 01 вересня 2014 року № 432 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08 лютого 2022 року № 66) основними завданнями територіального органу є:

1) забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку (далі – ДСУЗ), Національної системи конфіденційного зв'язку (далі – НСКЗ) та Національної телекомунікаційної мережі (далі – НТМ), реалізація державної політики у сферах криптографічного та технічного захисту інформації, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, протидії технічним розвідкам, у сферах захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у таких сферах;

2) участь у реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг (у частині контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг);

3) забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Територіальний орган відповідно до покладених на нього завдань:

1) забезпечує в регіоні функціонування, безпеку та розвиток ДСУЗ, її готовність до роботи в особливий період і в разі виникнення надзвичайної ситуації, а також у районі проведення антитерористичної операції;

2) забезпечує в регіоні в установленому законодавством порядку урядовим зв'язком Президента України, Голову Верховної Ради України, Прем'єр-міністра України, інших посадових осіб державних органів, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій в мирний час, в умовах надзвичайного стану і в особливий період;

3) забезпечує в регіоні функціонування, безпеку та розвиток НСКЗ;

4) здійснює будівництво і модернізацію НТМ, забезпечує її функціонування та надання послуг у зоні своєї відповідальності;

5) контролює в межах регіону виконання технічних умов та інших вимог законодавства у сфері захисту інформації у приміщеннях абонентів урядового зв'язку;

6) забезпечує в регіоні в установленому законодавством порядку та в межах компетенції діяльність суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом;

7) узагальнює та аналізує:

стан функціонування мереж і комплексів ДСУЗ, НСКЗ та НТМ у регіоні, готує та вносить пропозиції щодо їх удосконалення і подальшого розвитку;

результати здійснення державного контролю в регіоні за станом криптографічного та технічного захисту інформації, протидії технічним розвідкам і виконання вимог нормативно-правових актів у цих сферах; готує та надає Адміністрації Держспецзв'язку та державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до законів України, підприємствам, установам і організаціям рекомендації (пропозиції) щодо його поліпшення в регіоні;

інформацію щодо виконання необхідних захисних заходів у регіоні під час роботи іноземних інспекційних груп на території України на об'єктах інформаційної діяльності регіону, готує та вносить пропозиції щодо їх вдосконалення;

8) вирішує в межах повноважень питання забезпечення зв'язку для потреб ДСУЗ і НСКЗ згідно із законодавством;

9) бере участь у роботі спеціальних експертних комісій органів (підрозділів) Служби безпеки України з перевірки наявності умов для провадження діяльності, пов'язаної з державною таємницею, у державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях регіону, у складі яких є органи спеціального зв'язку;

10) бере участь (у межах своїх повноважень) у роботах, що проводяться Адміністрацією Держспецзв'язку, з реалізації державних цільових програм розвитку спеціальних видів зв'язку та захисту інформації;

11) бере участь у виконанні завдань із територіальної оборони, а також у заходах, спрямованих на підтримання в регіоні правового режиму воєнного та надзвичайного стану відповідно до закону;

12) реалізує у регіоні державну політику у сферах криптографічного та технічного захисту інформації, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, протидії технічним розвідкам;

13) реалізує в регіоні державну політику у сферах захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури;

14) координує в межах регіону діяльність суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

15) бере участь у межах своїх повноважень у реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг (у частині контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг);

16) координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури регіону на вразливість;

17) координує в регіоні діяльність щодо створення та проведення державної експертизи комплексних систем захисту інформації (далі – КСЗІ) в автоматизованих системах, які є одномашинними однокористувачевими комплексами (далі – АС класу «1»), відповідно до вимог нормативно-правових актів і нормативних документів з питань технічного захисту інформації (далі – ТЗІ), а також виконує такі функції:

розглядає та погоджує технічні завдання на створення КСЗІ в АС класу аналізує декларації про відповідність КСЗІ в АС класу «1» вимогам нормативних документів із ТЗІ;

забезпечує реєстрацію цих декларацій;

18) координує в регіоні діяльність щодо створення та атестації комплексів ТЗІ, що входять до складу КСЗІ в АС класу «1», та за окремим наказом Адміністрації Держспецзв'язку організаційно-розпорядчого характеру – на об'єктах інформаційної діяльності, де озвучується (озвучуватиметься) мовна інформація, що становить державну таємницю, відповідно до вимог нормативно-правових актів і нормативних документів

з питань ТЗІ. Також стосовно зазначених комплексів ТЗІ виконує такі функції:

розглядає та погоджує технічні завдання на створення комплексів ТЗІ;

розглядає та погоджує програми та методики атестації комплексів ТЗІ;

розглядає результати атестації комплексів ТЗІ;

забезпечує реєстрацію актів атестації комплексів ТЗІ;

19) виконує заходи за дозволом на проведення робіт із ТЗІ для власних потреб (за наявності) відповідно до розподілу обов'язків, що визначається рішенням Голови Держспецзв'язку;

20) організовує та забезпечує виконання заходів з протидії технічним розвідкам на об'єктах протидії, що перебувають у сфері його управління;

21) здійснює на території регіону контроль за виконанням технічних завдань на проєктування, будівництво і реконструкцію особливо важливих об'єктів і на розробку зразків військової та спеціальної техніки в частині протидії технічним розвідкам;

22) забезпечує в регіоні виконання завдань з мобілізаційної підготовки та мобілізаційної готовності держави;

23) здійснює державний контроль у регіоні за:

станом криптографічного та технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від форми власності, на об'єктах урядового зв'язку, а також під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України;

станом протидії технічним розвідкам у державних органах, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від їх підпорядкування та форми власності, які мають у своєму володінні, користуванні чи розпорядженні зразки озброєння, військової та спеціальної техніки, об'єкти оборонно-промислового комплексу, військові об'єкти та інші об'єкти, призначені для застосування в інтересах оборони і безпеки держави;

станом захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури;

дотриманням вимог законодавства у сфері електронних довірчих послуг;

додержанням вимог безпеки під час використання, експлуатації, вивезення та знищення засобів криптографічного захисту інформації та обладнання спеціального зв'язку, що має гриф обмеження доступу;

24) бере у межах своїх повноважень участь у погодженні питань розміщення на території регіону дипломатичних представництв і консульських установ іноземних держав;

25) здійснює контроль за охороною державної таємниці у структурних підрозділах територіального органу, організовує ведення діловодства;

26) бере участь у роботі комісій органів Служби безпеки України з перевірки стану охорони державної таємниці суб'єктів режимно-секретної діяльності, у складі яких функціонують органи спеціального зв'язку;

27) забезпечує охорону об'єктів, приміщень територіального органу, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації;

28) здійснює у взаємодії з відповідними структурними підрозділами Адміністрації Держспецзв'язку матеріально-технічне, кадрове, фінансове і правове забезпечення діяльності територіального органу; організовує спільно з Медичним центром Держспецзв'язку медичне забезпечення військовослужбовців територіального органу;

29) забезпечує відповідно до законодавства правовий і соціальний захист військовослужбовців територіального органу і членів їхніх сімей;

30) забезпечує в межах своїх повноважень виконання заходів з охорони праці та пожежної безпеки на об'єктах, що перебувають у сфері управління територіального органу;

31) вживає в межах своїх повноважень виконання заходів щодо запобігання та виявлення корупції серед особового складу територіального органу;

32) здійснює добір кадрів, організовує роботу з підготовки, перепідготовки й підвищення кваліфікації особового складу територіального органу;

33) видає в межах своїх повноважень накази організаційно-розпорядчого характеру;

34) за рішенням Адміністрації Держспецзв'язку виступає в регіоні замовником будівництва житла та інших об'єктів Держспецзв'язку, вживає заходів щодо їх експлуатації, реконструкції та ремонту;

35) веде облік військовослужбовців, які потребують забезпечення житлом та/або поліпшення житлових умов, формує фонд службового житла, вживає заходів щодо забезпечення житлом військовослужбовців територіального органу;

36) організовує і веде бухгалтерський і податковий облік у порядку, що встановлений для бюджетних організацій; складає і подає статистичну, фінансову, бюджетну і податкову звітність у порядку й у терміни, встановлені законодавством;

37) забезпечує ефективне, результативне і цільове використання бюджетних коштів;

38) організовує планово-фінансову роботу, здійснює контроль за використанням фінансових і матеріальних ресурсів, забезпечує організацію та вдосконалення бухгалтерського обліку;

39) веде перелік об’єктів державної власності, що знаходяться в його оперативному управлінні, та подає інформацію щодо цих об’єктів до Адміністрації Держспецзв’язку;

40) забезпечує цільове використання, ефективну експлуатацію та утримання земельних ділянок, адміністративних та господарських будівель, стаціонарних технічних засобів та інженерних споруд, інших об’єктів, у тому числі комунального призначення, та іншого майна, що перебувають в оперативному управлінні територіального органу.

<u>Територіальні підрозділи ДССЗЗІ України</u>

входять до загальної структури ДССЗЗІ України, підпорядковуються Адміністрації Держспецзв’язку і забезпечують виконання покладених на них завдань відповідно до затвердженого Головою Державної служби спеціального зв’язку та захисту інформації України “Положення про територіальний підрозділ ДССЗЗІ України”

Територіальні підрозділи Державної служби спеціального зв’язку та захисту інформації України призначені для:

організації та забезпечення стійкого функціонування урядового зв’язку Президента України як Верховного Головнокомандувача Збройних Сил України з посадовими особами Збройних Сил України, інших військових формувань, утворених відповідно до законів України, правоохоронних органів спеціального призначення під час їх перебування на захищених і польових пунктах управління у мирний час, в умовах надзвичайного стану та в особливий період;

забезпечення функціонування, безпеки та розвитку підсистеми урядового польового зв’язку як складової державної системи урядового зв’язку.

Мобілізаційне розгортання і приведення у готовність територіальних підрозділів Державної служби спеціального зв’язку та захисту інформації України для функціонування в особливий період здійснюються відповідно до планів, які розробляються центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку, захисту інформації, погоджуються з Генеральним штабом Збройних Сил України та затверджуються Головою Державної служби спеціального зв’язку та захисту інформації України.

Отже, на Державну службу спеціального зв’язку та захисту інформації України, а також її підпорядковані структурні підрозділи покладені багатовекторні завдання у різних секторах забезпечення

інформаційної безпеки, які займають важливе місце у забезпеченні не тільки інформаційної, а й національної безпеки держави вцілому.

Ці завдання спрямовані на:

1) забезпечення формування та реалізації державної політики у сферах:

криптографічного і технічного захисту інформації;

поштового зв'язку спеціального призначення;

урядового фельд'єгерського зв'язку;

захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності;

використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам;

функціонування, безпеки та розвитку Національної телекомунікаційної мережі, державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

забезпечення безпеки державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в кіберпросторі, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

2) участь у формуванні та реалізації (разом з іншими суб'єктами ІБ держави):

державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), захисту критичної інформаційної інфраструктури, електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг);

3) реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю у зазначених сферах.

В підрозділах розділів 2 та 3 будуть розглянуті положення відповідних НПА, які регламентують організацію та впровадження заходів у визначених сферах повноважень Державної служби спеціального зв'язку та захисту інформації України.

1.6.4 Повноваження юридичних осіб та громадян України

В сучасному інформаційному просторі повноваження фізичних та юридичних осіб, як суб’єктів інформаційних відносин та інформаційної безпеки держави, окреслені положеннями Конституції України, законодавчих та нормативно-правових актів концептуального та конститутивного рівнів у сфері ІБ, головні із яких ми вже розглянули.

Загальні положення щодо повноважень цих суб’єктів можна сформулювати наступним чином:

Відповідно до положень Конституції України: [8]

Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави.

Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави *(стаття 3)*.

Державною мовою в Україні є українська мова.

Держава забезпечує всебічний розвиток і функціонування української мови в усіх сферах суспільного життя на всій території України.

В Україні гарантується вільний розвиток, використання і захист російської, інших мов національних меншин України.

Держава сприяє вивченню мов міжнародного спілкування.

Застосування мов в Україні гарантується Конституцією України та визначається законом *(стаття 10)*.

Держава сприяє консолідації та розвиткові української нації, її історичної свідомості, традицій і культури, а також розвиткові етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України *(стаття 11).*

Україна дбає про задоволення національно-культурних і мовних потреб українців, які проживають за межами держави *(стаття 12)*.

Держава забезпечує захист прав усіх суб'єктів права власності й господарювання, соціальну спрямованість економіки. Усі суб'єкти права власності рівні перед законом *(стаття 13)*.

Суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності.

Жодна ідеологія не може визнаватися державою як обов'язкова.

Цензура заборонена.

Держава гарантує свободу політичної діяльності, не забороненої Конституцією і законами України *(стаття 15).*

Правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством *(стаття 15).*

Усі люди є вільні й рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними *(стаття 21)*.

Права і свободи людини і громадянина, закріплені цією Конституцією, не є вичерпними.

Конституційні права і свободи гарантуються і не можуть бути скасовані.

У разі прийняття нових законів або внесення змін до чинних законів не допускається звуження змісту та обсягу наявних прав і свобод *(стаття 22)*.

Кожна людина має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та має обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості *(стаття 23)*.

Громадяни мають рівні конституційні права і свободи та є рівними перед законом.

Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками.

Рівність прав жінки й чоловіка забезпечується: наданням жінкам рівних з чоловіками можливостей у громадсько-політичній і культурній діяльності, у здобутті освіти і професійній підготовці, у праці та винагороді за неї; спеціальними заходами щодо охорони праці й здоров'я жінок, встановленням пенсійних пільг; створенням умов, які дають жінкам можливість поєднувати працю з материнством; правовим захистом, матеріальною і моральною підтримкою материнства і дитинства, включаючи надання оплачуваних відпусток та інших пільг вагітним жінкам і матерям *(стаття 24)*.

Громадянин України не може бути позбавлений громадянства і права змінити громадянство.

Громадянин України не може бути вигнаний за межі України або виданий іншій державі.

Україна гарантує піклування та захист своїм громадянам, які перебувають за її межами *(стаття 25)*.

Іноземці та особи без громадянства, що перебувають в Україні на законних підставах, користуються тими самими правами і свободами, а також несуть такі самі обов'язки, як і громадяни України, – за винятками, встановленими Конституцією, законами чи міжнародними договорами України.

Іноземцям та особам без громадянства може бути надано притулок у порядку, встановленому законом *(стаття 26)*.

Кожен має право на повагу до його гідності.

Ніхто не може бути підданий катуванню, жорстокому, нелюдському або такому, що принижує його гідність, поводженню чи покаранню.

Жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідам *(стаття 28)*.

Кожна людина має право на свободу та особисту недоторканність.

Ніхто не може бути заарештований або триматися під вартою інакше як за вмотивованим рішенням суду і тільки на підставах та в порядку, встановлених законом *(стаття 29)*.

Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо *(стаття 31)*.

Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування

матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації *(стаття 32)*.

Кожному, хто на законних підставах перебуває на території України, гарантується свобода пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом.

Громадянин України не може бути позбавлений права в будь-який час повернутися в Україну *(стаття 33)*.

Кожному гарантується право на свободу думки й слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя *(стаття 34)*.

Кожен має право на свободу світогляду й віросповідання. Це право включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноосібно чи колективно релігійні культи й ритуальні обряди, вести релігійну діяльність.

Здійснення цього права може бути обмежене законом лише в інтересах охорони громадського порядку, здоров'я і моральності населення або захисту прав і свобод інших людей.

Церква і релігійні організації в Україні відокремлені від держави, а школа – від церкви. Жодна релігія не може бути визнана державою як обов'язкова.

Ніхто не може бути увільнений від своїх обов'язків перед державою або відмовитися від виконання законів за мотивами релігійних переконань. У разі якщо виконання військового обов'язку суперечить релігійним переконанням громадянина, виконання цього обов'язку має бути замінене альтернативною (невійськовою) службою *(стаття 35)*.

Громадяни України мають право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів, за винятком обмежень, встановлених законом в інтересах

національної безпеки та громадського порядку, охорони здоров'я населення або захисту прав і свобод інших людей.

Політичні партії в Україні сприяють формуванню і вираженню політичної волі громадян, беруть участь у виборах. Членами політичних партій можуть бути лише громадяни України. Обмеження щодо членства у політичних партіях встановлюються виключно цією Конституцією і законами України.

Громадяни мають право на участь у професійних спілках з метою захисту своїх трудових і соціально-економічних прав та інтересів. Професійні спілки є громадськими організаціями, що об'єднують громадян, пов'язаних спільними інтересами за родом їх професійної діяльності. Професійні спілки утворюються без попереднього дозволу на основі вільного вибору їх членів. Усі професійні спілки мають рівні права. Обмеження щодо членства у професійних спілках встановлюються виключно цією Конституцією і законами України.

Ніхто не може бути примушений до вступу в будь-яке об'єднання громадян чи обмежений у правах за належність чи неналежність до політичних партій або громадських організацій.

Усі об'єднання громадян рівні перед законом *(стаття 36)*.

Утворення і діяльність політичних партій та громадських організацій, програмні цілі або дії яких спрямовані на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, на розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров'я населення, *забороняються.*

Політичні партії та громадські організації *не можуть мати воєнізованих формувань.*

Не допускається створення і діяльність організаційних структур політичних партій в органах виконавчої та судової влади і виконавчих органах місцевого самоврядування, військових формуваннях, а також на державних підприємствах, у навчальних закладах та інших державних установах і організаціях.

Заборона діяльності об'єднань громадян здійснюється лише в судовому порядку *(стаття 37)*.

Громадяни мають право брати участь в управлінні державними справами, у всеукраїнському та місцевих референдумах, вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування.

Громадяни користуються рівним правом доступу до державної служби, а також до служби в органах місцевого самоврядування *(стаття 38).*

Усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк *(стаття 40).*

Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності.

Право приватної власності набувається в порядку, визначеному законом.

Громадяни для задоволення своїх потреб можуть користуватися об'єктами права державної та комунальної власності відповідно до закону *(стаття 41).*

Кожен має право на підприємницьку діяльність, яка не заборонена законом.

Підприємницька діяльність депутатів, посадових і службових осіб органів державної влади та органів місцевого самоврядування обмежується законом.

Держава забезпечує захист конкуренції у підприємницькій діяльності. Не допускаються зловживання монопольним становищем на ринку, неправомірне обмеження конкуренції та недобросовісна конкуренція. Види і межі монополії визначаються законом.

Держава захищає права споживачів, здійснює контроль за якістю і безпечністю продукції та усіх видів послуг і робіт, сприяє діяльності громадських організацій споживачів *(стаття 42).*

Кожен має право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди.

Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена *(стаття 50).*

Кожен має право на освіту.

Повна загальна середня освіта є обов'язковою.

Держава забезпечує доступність і безоплатність дошкільної, повної загальної середньої, професійно-технічної, вищої освіти в державних і комунальних навчальних закладах; розвиток дошкільної, повної загальної середньої, позашкільної, професійно-технічної, вищої і післядипломної освіти, різних форм навчання; надання державних стипендій та пільг учням і студентам.

Громадяни мають право безоплатно здобути вищу освіту в державних і комунальних навчальних закладах на конкурсній основі.

Громадянам, які належать до національних меншин, відповідно до закону гарантується право на навчання рідною мовою чи на вивчення рідної мови у державних і комунальних навчальних закладах або через національні культурні товариства *(стаття 53).*

Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності.

Кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом.

Держава сприяє розвиткові науки, встановленню наукових зв'язків України зі світовим співтовариством.

Культурна спадщина охороняється законом.

Держава забезпечує збереження історичних пам'яток та інших об'єктів, що становлять культурну цінність, вживає заходів для повернення в Україну культурних цінностей народу, які знаходяться за її межами *(стаття 54).*

Права і свободи людини і громадянина захищаються судом.

Кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб.

Кожен має право звертатися за захистом своїх прав до Уповноваженого Верховної Ради України з прав людини.

Кожному гарантується право звернутись із конституційною скаргою до Конституційного Суду України з підстав, установлених цією Конституцією, та у порядку, визначеному законом *(стаття 55).*

Кожному гарантується право знати свої права і обов'язки.

Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення у порядку, встановленому законом.

Закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними *(стаття 57).*

Закони та інші нормативно-правові акти не мають зворотної дії в часі, крім випадків, коли вони пом'якшують або скасовують відповідальність особи.

Ніхто не може відповідати за діяння, які на час їх вчинення не визнавалися законом як правопорушення *(стаття 58).*

Ніхто не зобов'язаний виконувати явно злочинні розпорядження чи накази.

За віддання і виконання явно злочинного розпорядження чи наказу настає юридична відповідальність *(стаття 60).*

Конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України.

В умовах воєнного або надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень *(стаття 64).*

Кожен зобов'язаний не заподіювати шкоду природі, культурній спадщині, відшкодовувати завдані ним збитки *(стаття 66).*

Кожен зобов'язаний неухильно додержуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей.

Незнання законів не звільняє від юридичної відповідальності *(стаття 68).*

Відповідно до положень Закону України "Про інформацію": [12]

Стаття 5. Право на інформацію

Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Стаття 6. Гарантії права на інформацію

1. Право на інформацію забезпечується:

створенням механізму реалізації права на інформацію;

створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

обов'язком суб'єктів владних повноважень інформувати громадськість та засоби масової інформації про свою діяльність і прийняті рішення;

обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

здійсненням державного й громадського контролю за додержанням законодавства про інформацію;

встановленням відповідальності за порушення законодавства про інформацію.

2. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 7. Охорона права на інформацію

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Заборонено вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

Стаття 8. Мова інформації

Мову інформації визначають Закон України “Про забезпечення функціонування української мови як державної”, інші закони України та міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

Стаття 9. Основні види інформаційної діяльності

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Повноваження фізичних та юридичних осіб можуть уточнюватись та розширюватись без зміни конституційних основ положеннями інших законодавчих та нормативно-правових актів концептуального та конститутивного рівнів у сфері ІБ.

Отже, у положеннях НПА, які складають систему нормативно-правового забезпечення України, усім суб'єктам ІБ на юридичному рівні визначені відповідні повноваження. Окрім загальних напрямків діяльності щодо забезпечення ІБ держави кожному суб'єкту визначені (відповідно до його місця в загальній класифікації) індивідуальні повноваження, права та обов'язки, а також і відповідальність за їх виконання та можливі порушення встановлених законодавством України вимог у сфері ІБ.

1.7. Відповідальність осіб за порушення встановлених законодавством України вимог у сфері ІБ

У процесі вивчення положень чинних нормативно-правових актів ми постійно акцентували увагу на встановленій законодавством України відповідальності суб'єктів інформаційних відносин та інформаційної безпеки за порушення встановлених вимог в цій сфері діяльності.

Залежно від категорії порушень, негативних наслідків та завданих збитків державі встановлено ***юридичну відповідальність осіб***.

Юридична відповідальність – це застосування до особи, яка вчинила правопорушення, примусових заходів у встановленому законодавством процесуальному порядку.

У контексті змісту цієї глави наведемо конкретні положення раніше вивчених НПА.

Так, у положеннях Закону України *"Про інформацію"* визначено:

"Стаття 27. Відповідальність за порушення законодавства про інформацію

Порушення законодавства України про інформацію тягне за собою ***дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність*** *згідно із законами України".* [12]

Закон України *"Про захист інформації в інформаційно-комунікаційних системах"* також встановлює, що відповідальність за порушення законодавства про захист інформації в ІС полягає у притягненні ***до дисциплінарної, цивільно-правової, адміністративної та кримінальної відповідальності***.

Подібні положення щодо відповідальності осіб за порушення встановлених законодавством України вимог у сфері ІБ містять й інші базові закони України, які встановлюють правила відносин суб'єктів у певних секторах ІБ держави.

Положення законодавчих норм щодо встановлення певних видів відповідальності за порушення встановлених законодавством держави вимог у сфері ІБ реалізуються через положення статей відповідних ***Кодексів України***.

Розглянемо деякі з них.

"Кодекс законів про працю України" *(в редакції від 24 грудня 2023 року № 3494-IX)* юридично обґрунтовує ***дисциплінарну відповідальність*** посадових осіб підприємств, організацій та установ усіх форм власності. Дисциплінарні стягнення накладає адміністрація підприємств, установ, організацій (особа, що має розпорядчо-дисциплінарну владу над конкретним працівником) унаслідок вчинення посадовими особами дисциплінарних порушень:

1) відповідно до правил внутрішнього трудового розпорядку;

2) у порядку підпорядкованості;

3) відповідно до дисциплінарних статутів і положень.

До *дисциплінарної відповідальності притягаються посадові особи установ, що вчинили правопорушення у сфері ЗБІ, але тяжкість наслідків такого правопорушення не передбачає кримінальної або адміністративної відповідальності.* Дисциплінарна відповідальність передбачає накладання встановленим порядком рішенням керівника установи на винну особу таких стягнень, як: *"догана", "звільнення".*

Цивільно-правова відповідальність має юридичною підставою ***Цивільно-процесуальний Кодекс України*** *(в редакції від 23 червня 2005 року № 2709-IV)***.**

Цивільно-правова відповідальність полягає в застосуванні до правопорушника в інтересах іншої сторони (установи або держави) установлених законом або договором правових заходів упливу, що має для нього негативні, економічно невигідні наслідки майнового характеру, а саме: *відшкодування збитків, штраф, відшкодування шкоди тощо.*

Адміністративна відповідальність за вчинення правопорушень, зокрема тих, що пов'язані з одержанням, використанням, поширенням та зберіганням інформації, регламентується ***Кодексом України про адміністративні правопорушення*** *(в редакції від 13 липня 2023 року № 3234-IX).* [30]

Справи про адміністративні правопорушення розглядаються органами внутрішніх справ, інспекціями у справах неповнолітніх, митними органами, судами, іншими державними органами й посадовими особами, які уповноважені на те законом.

Так, згідно зі статтею 188-31 “Невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України”, порушення законодавства стосовно криптографічного та технічного захисту інформації, яка належить державі, або обмеженої інформації, а також невиконання вимог щодо послуг електронного цифрового підпису, і створення перешкод для виконання обов'язків посадовими особами органів Державної служби спеціального зв'язку та захисту інформації України, тягне за собою накладення штрафу на посадових осіб від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.

Ті самі дії, вчинені повторно протягом року після накладення адміністративного стягнення, тягнуть за собою накладення штрафу на посадових осіб від ста до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Стаття 188-39 “Порушення законодавства у сфері захисту персональних даних”.

Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб’єкта персональних даних тягне за собою накладення штрафу на громадян від ста до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян-суб’єктів підприємницької діяльності, – від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню, тягне за собою накладення штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян.

Підставою для ***кримінальної відповідальності*** є вчинення особою суспільно небезпечного діяння, яке містить склад кримінального правопорушення, передбаченого ***“Кримінальним кодексом України”*** *(в редакції від 28 березня 2024 року № 2341-III)*.

Кримінальна відповідальність у вигляді конкретного покарання є заходом примусу, що застосовується від імені держави за вироком суду до особи, визнаної винною у вчиненні кримінального правопорушення, і полягає в передбаченому законом обмеженні прав і свобод засудженого.

До осіб, визнаних винними у вчиненні кримінального правопорушення, судом можуть бути застосовані такі види покарань:

1) штраф;

2) позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу;

3) позбавлення права обіймати певні посади або займатися певною діяльністю;

4) громадські роботи;

5) виправні роботи;

6) службові обмеження для військовослужбовців;

7) конфіскація майна;

8) арешт;

9) обмеження волі;

10) тримання в дисциплінарному батальйоні військовослужбовців;

11) позбавлення волі на певний строк;

12) довічне позбавлення волі.

Щодо положень ***"Кримінального кодексу України"*** розглянемо положення наступних статей, в яких визначається склад злочину у сфері ІБ держави та встановлюється кримінальна відповідальність осіб: [29]

Стаття 182 "Порушення недоторканності приватного життя".

Порушення недоторканності приватного життя караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

Аналогічні дії протягом року після покарання – караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк.

Стаття 114. Шпигунство

Передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства, – караються позбавленням волі на строк від восьми до п'ятнадцяти років.

Звільняється від кримінальної відповідальності особа, яка припинила діяльність, передбачену частиною першою цієї статті, та добровільно повідомила органи державної влади про вчинене, якщо внаслідок цього і вжитих заходів було відвернено заподіяння шкоди інтересам України.

Стаття 328. Розголошення державної таємниці

Розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з

виконанням службових обов’язків, за відсутності ознак державної зради або шпигунства, – карається позбавленням волі на строк від двох до п’яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Те саме діяння, якщо воно спричинило тяжкі наслідки, – карається позбавленням волі на строк від п’яти до восьми років.

Стаття 329. Втрата документів, що містять державну таємницю

Втрата документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами, – карається позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Те саме діяння, якщо воно спричинило тяжкі наслідки, – карається позбавленням волі на строк від двох до п’яти років.

Стаття 330. Передача або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави

Передача або збирання з метою передачі іноземним підприємствам, установам, організаціям або їх представникам економічних, науково-технічних або інших відомостей, що становлять конфіденційну інформацію, яка є власністю держави, особою, якій ці відомості були довірені або стали відомі у зв’язку з виконанням службових обов’язків, за відсутності ознак державної зради або шпигунства, – караються обмеженням волі на строк до трьох років або позбавленням волі на строк від двох до п’яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Ті самі дії, вчинені з корисливих мотивів, або такі, що спричинили тяжкі наслідки для інтересів держави, або вчинені повторно, або за попередньою змовою групою осіб, – караються позбавленням волі на строк від чотирьох до восьми років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Стаття 363. “Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється”.

Порушення вищезазначених правил карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Отже, в державі відповідно до положень Конституції на законодавчому рівні упроваджений порядок визначення певних видів відповідальності суб'єктів інформаційних відносин за порушення встановлених вимог у сфері ІБ. Цей порядок реалізуються через положення статей відповідних Кодексів України.

Наведений вище зміст статей та положень Кодексів України яскраво переконує в наступному: задля уникнення відповідальності суб'єкти ІБ зобов'язані ретельно виконувати всі вимоги, норми та положення у сфері ІБ держави, встановлені відповідними нормативно-правовими актами України.

Висновки по розділу 1.

У змісті пунктів розділу 1 проаналізовано вітчизняну систему нормативно-правового забезпечення ІБ, напрями державної політики в цій сфері, розглянуто структуру та повноваження суб'єктів, що забезпечують інформаційну безпеку в Україні.

Сфера інформаційної безпеки держави містить чималу кількість відповідних термінів, визначень та понять, розуміння суті яких забезпечує успішне засвоєння здобувачами вищої освіти навчального матеріалу даного освітнього компонента.

Система нормативно-правового забезпечення ІБ в державі закладає конституційні норми інформаційних відносин у суспільстві (між його членами й державою, між фізичними та юридичними особами), основні принципи відповідних відносин на міждержавному рівні, а також передбачає відповідальність суб'єктів за порушення встановлених законодавством України вимог в цій сфері.

Систему нормативно-правових актів України у сфері інформаційної безпеки доцільно розглядати за такими класифікаційними ознаками: *рівень ієрархії (юридичної сили), сфера (сектор ІБ) застосування, призначення та зміст НПА та нормативних документів.*

Класифікація *за ієрархією* визначає фундаментальні підходи до визначення юридичної сили тих чи інших нормативних актів України. Суб'єкти інформаційних відносин повинні враховувати ієрархію (юридичну силу) НПА, а також чинне законодавство України у сфері ЗІБ та захисту інформації під час розробки та впровадження власних нормативних та організаційно-розпорядчих документів з цих питань.

Класифікація чинних законодавчих, нормативно-правових актів та нормативних документів за ознакою *сфера застосування (сектор ІБ)* надає можливості вивчення їхніх положень та системного формування знань,

необхідних для виконання завдань у певному секторі ІБ відповідно до покладених на фахівців посадових обов'язків. А в разі переміщення по службі на інші сектори ІБ, швидко орієнтуватись щодо напрямку та обсягу нарощування своїх професійних знань та адаптації на новій посаді в іншому відділі, управлінні або іншій установі.

Класифікація *за назвою та приналежністю* нормативного документа до певного виду надає можливість фахівцям пришвидшити пошук необхідних положень НПА для обґрунтованого виконання певних службових завдань.

Законодавчі та нормативно-правові акти концептуального рівня є законодавчою основою для НПА конститутивного та інституційного рівнів. Таким чином, в системі нормативно-правового забезпечення інформаційної безпеки створена чітка вертикаль НПА за рівнем їхньої юридичної сили. На першому рівні маємо Конституцію України, закони, акти та положення, які визначають та закріплюють концептуальні положення. На другому рівні знаходяться НПА конститутивного рівня. Вони закріплюють визначальні положення щодо ЗІБ України та захисту інформації.

Положення НПА інституційного рівня мають спрямованість на практичне покрокове виконання вимог з забезпечення кібербезпеки в певних установах та організаціях. Саме в їхній практичній спрямованості полягає головна відмінність їхнього призначення порівняно з НПА концептуального та конститутивного рівнів ієрархії. Вони є певною ланкою у системі НПА, на положеннях яких ґрунтуються вимоги інших нормативних документів суто практичного застосування, а саме: методик, правил, інструкцій, порядків, методичних вказівок, рекомендацій тощо.

Знання принципів побудови системи нормативно-правових актів України у сфері інформаційної безпеки озброює здобувачів певним інструментом подальшого системного вивчення положень чинних НПА та нормативних документів в цій сфері, сприяє формуванню у них професійних знань, відповідних компетентностей фахівців ДССЗЗІ України.

Прагнення України долучитися до інформаційного простору світової демократичної спільноти, і насамперед країн Європейського Союзу, зумовлює інтеграцію міжнародних стандартів та норм інформаційної безпеки в національну систему нормативно-правового забезпечення ІБ України. Цей динамічний процес складає передумови успішного вирішення завдань, покладених на суб'єкти ІБ, як на міжнародній арені, так і всередині держави.

Кожний із розглянутих у посібнику міжнародних стандартів має своє призначення та місце в переліку головних НПА держави. Вони адаптовані в загальну систему нормативно-правового забезпечення ІБ держави з метою досягнення максимального наближення до вимог та норм, які є

загальноприйнятими для усіх країн-членів ЄС та НАТО, а також забезпечення участі України в загальноєвропейській та регіональній системах колективної безпеки, міжнародних проєктах економічної, політичної, екологічної, гуманітарної, миротворчої та інших видів діяльності під егідою ООН та ОБСЄ.

Напрямки роботи щодо забезпечення інформаційної безпеки держави є багатовекторними, вони стосуються діяльності різних суб'єктів інформаційних відносин та охоплюють різні сфери функціонування держави: зовнішньополітичну, внутрішньополітичну, економічну, сферу державної безпеки та оборони, соціальну, гуманітарну екологічну тощо.

У положеннях НПА, які складають систему нормативно-правового забезпечення України, усім суб'єктам ІБ на юридичному рівні визначені відповідні повноваження та завдання.

Певне місце у цій роботі відведено Державній службі спеціального зв'язку та захисту інформацій. На законодавчому рівні їй надано певні повноваження та визначено важливі завдання у сфері інформаційної безпеки. Ці завдання можна згрупувати у певну кількість напрямків діяльності ДССЗЗІ України, тобто накреслити дорожню карту, за якою здобувачам вищої освіти належить розпочати системне вивчення нормативно-правового забезпечення інформаційної безпеки в державі.

У державі відповідно до положень Конституції на законодавчому рівні упроваджено порядок визначення певних видів відповідальності суб'єктів інформаційних відносин за порушення встановлених вимог в сфері ІБ. Цей порядок реалізуються через положення статей відповідних Кодексів України.

Наведений у цьому розділі зміст статей та положень Кодексів України яскраво переконують в наступному: задля уникнення відповідальності посадові особи суб'єктів ІБ зобов'язані ретельно виконувати всі вимоги, норми та положення у сфері ІБ держави, встановлені відповідними нормативно-правовими актами України.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ (ПРОВЕДЕННЯ ПОТОЧНОГО КОНТРОЛЮ)

1. Що мається на увазі під термінами "інформація", "інформаційний суверенітет", "інформаційна безпека"?
2. Який нормативно-правовий акт України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері в сучасних умовах?

3. Що належить до життєво важливих інтересів громадянина держави (особи) і є одним із важливих національних інтересів України в інформаційній безпеці?

4. Що належить до об’єктів забезпечення ІБ держави?

5. На які категорії поділяються законодавчі та нормативно-правові акти держави в сфері забезпечення ІБ за їх ієрархією?

6. Яке місце займає ІБ у переліку напрямків діяльності щодо забезпечення національної безпеки держави (відповідно до положень Конституції України (Основного Закону) від 28 червня 1996 року № 254к/96-ВР (зі змінами))?

7. Доповісти про основні принципи інформаційних відносин у державі (відповідно до положень Закону України “Про інформацію” від 02 жовтня 1992 року № 2657-XII (зі змінами)).

8. Доповісти про призначення та основні положення:

нормативно-правових актів: “Доктрина інформаційної безпеки України” (введена в дію указом Президента України від 25 лютого 2016 року № 47/2017); “Стратегія інформаційної безпеки” (введена в дію указом Президента України від 28 грудня 2021 року № 685/2021);

Законів України “Про захист інформації в інформаційно-комунікаційних системах” від 05 липня 1994 року № 80/94-ВР (зі змінами), “Про електронні комунікації” від 16 грудня 2020 року № 1089-IX (зі змінами), “Про електронні документи та електронний документообіг” від 22 травня 2003 року № 851-IV (зі змінами), “Про захист персональних даних” від 01 червня 2010 року № 2297-VI (зі змінами) , “Про Національну систему конфіденційного зв'язку” від 10 січня 2002 року № 2919-III (зі змінами), “Про державну таємницю” від 21 січня 1994 року № 3856-XII (зі змінами).

9. Що є об'єктом (ами) захисту в ІКС (відповідно до положень Закону України “Про захист інформації в інформаційно-комунікаційних системах” від 05 липня 1994 року № 80/94-ВР)?

10. Що маємо на увазі під терміном “електронний документ” (надати пояснення відповідно до положень Закону України “Про електронні документи та електронний документообіг” від 22 травня 2003 року № 851-IV)?

11. Хто є суб'єктами відносин, пов'язаних із персональними даними (відповідно до положень Закону України “Про захист персональних даних” від 01 червня 2010 року № 2297-VI)?

12. Доповісти про призначення та основні положення:

Законів України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 року № 2163-VIII (зі змінами); “Про критичну інфраструктуру” від 16 листопада 2021 року № 1882-IX (зі змінами);

нормативно-правових актів: “Стратегія кібербезпеки України” (указ Президента України від 26 серпня 2021 року № 447/2021); “Загальні

вимоги до кіберзахисту об’єктів критичної інфраструктури” (постанова Кабінету Міністрів України від 19 червня 2019 року № 518).

13. Надати визначення термінам “кіберпростір” “кібербезпека”, “кіберзагроза”, “кіберзахист”, “кіберзлочин”, “кібероборона”, “критична інформаційна інфраструктура”.

14. Що є першочерговими пріоритетами забезпечення кібербезпеки України відповідно до положень “Стратегії кібербезпеки України” (указ Президента України від 26 серпня 2021 року № 447/2021)?

15. Скільки та які категорії критичності об'єктів критичної інфраструктури встановлені Законом України “Про критичну інфраструктуру” від 16 листопада 2021 року № 1882-IX (зі змінами)?

16. Якими шляхами забезпечується кіберзахист об’єктів критичної інфраструктури держави (відповідно до положень постанови КМУ від 19 червня 2019 року № 518 “Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури”)?

17. Пояснити, у чому полягає суть інтеграційних процесів нормативно-правових актів України з міжнародними стандартами та вимогами в галузі інформаційної безпеки?

18. Доповісти про призначення та спрямованість положень міжнародних стандартів SO/IEC 27001, ISO/IEC 27002, ISO/IEC 9798-1:2002, ISO/IEC 9798-3:2002.

19. Доповісти про загальну класифікацію та головні повноваження суб’єктів забезпечення ІБ України.

20. Доповісти про повноваження та завдання Державної служби спеціального зв’язку та захисту інформації України щодо забезпечення ІБ держави.

21. Доповісти про повноваження юридичних осіб та громадян України щодо забезпечення ІБ держави.

22. До якої відповідальності та на підставі положень яких НПА можуть бути притягнуті особи за порушення встановлених законодавством України вимог в сфері ІБ?

Розділ 2
ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1 Положення основних нормативно правових актів України щодо забезпечення захисту інформації в інформаційних та інформаційно-комунікаційних системах

Як відомо зі змісту Розділу 1 цього посібника, саме в положеннях Закону України "Про захист інформації в інформаційно-теле-комунікаційних системах" від 05 липня 1994 року № 80/94-ВР, (зі змінами) встановлені обов'язкові умови щодо забезпечення безпеки державних інформаційних ресурсів, а також інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом (стаття 8 Закону). Суть цих умов полягає у наявності в таких ІКС *комплексної системи захисту інформації з підтвердженою відповідністю*.

Ці положення статті 8 Закону в непідготовленої особи відразу генерують цілу низку питань, а саме: що таке КСЗІ, які технології захисту вона повинна реалізовувати, який перелік цих технологій захисту (комплекс засобів захисту), від яких чинників залежить і як обґрунтувати достатню потребу в них залежно від важливості інформації, яка підлягає обробці; чи можливо впровадити КСЗІ, якщо вже існує певна ІКС, якщо – ні, то коли потрібно впроваджувати КСЗІ; які етапи її створення, яких фінансових та фізичних витрат потребує побудова КСЗІ, що означає "підтверджена відповідність КСЗІ"; хто із суб'єктів інформаційних відносин уповноважений її "підтвердити", а сам процес "підтвердження відповідності КСЗІ" наскільки є складним, скільки часу він буде тривати, який очікуваний термін проведення атестації КСЗІ та можливості розпочати обробку інформації в ІКС, як забезпечити захист інформації в ІКС в процесі її експлуатації, чи є встановлені для цього правила? Цей перелік суто практичних питань можна продовжити далі.

Для надання відповідей на ці та інші питання необхідно розглянути систему НПА та нормативних документів, що діють в цьому секторі ІБ.

Положення статті 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" стануть відправною точкою для пошуку відповідей на вище сформульовані питання, системного вивчення положень чинних НПА та набуття первинних базових професійних знань з питань ***забезпечення захисту інформації в інформаційно-комунікаційних системах.***

В подальшому ці базові знання здобувачів вищої освіти зі спеціальності 125 *Кібербезпека та захист інформації* стануть підгрунттям

для успішного вивчення навчального матеріалу із освітніх компонент “Технічний захист інформації”, “Системи та комплекси технічного захисту інформації”, “Убезпечення інформації від витоку технічними каналами”, “Основи спеціальних досліджень”, “Інструментальний контроль об’єктів інформаційної діяльності”.

Як і будь-який інший сектор інформаційної безпеки, сектор, пов'язаний із забезпеченням захисту інформації в інформаційних та інформаційно-комунікаційних системах, має певну систему НПА та нормативних документів із властивою для цієї специфіки термінологією.

Накопичення професійних знань починається із вивчення спеціальних термінів та понять, чинних у сфері функціонування автоматизованих систем та технологій обробки інформації в них, які встановлені відповідними державними стандартами.

2.1.1 ДСТУ 2226-93 “Автоматизовані системи. Терміни та визначення”

Державний стандарт України 2226-93 “Автоматизовані системи. Терміни та визначення” (далі – ДСТУ 2226-93) був уведений в дію з 01 липня 1994 року і на теперішній час є чинним.

ДСТУ 2226-93 встановлює терміни та визначення основних понять у галузі автоматизованих систем (АС) та поширюється на АС, які використовуються в різних сферах діяльності людини (керування, дослідження, проєктування тощо), метою яких є обробка інформації. [31]

Стандарт не поширюється на терміни та визначення в галузі АС, призначені для безпосереднього оброблення (виготовлення, зберігання, транспортування) будь-яких виробів, матеріалів або енергії.

Терміни, установлені цим стандартом, обов’язкові для використання в усіх видах документації та літератури, що входять у сферу робіт зі стандартизації, та рекомендовані для використання в науково-технічній, навчальній і довідковій літературі та в комп’ютерних інформаційних системах.

Для кожного поняття установлено один стандартизований термін.

Для окремих стандартизованих термінів наведено короткі форми, які дозволено вживати у випадках, що виключають неоднозначність їх тлумачення.

Загальна кількість термінів, наведених у стандарті – 247. Для зручності користування всі терміни за тематичною ознакою зведені до 9 розділів. Кожний розділ стандарту має свою тематичну назву, наприклад: 1 – Загальні поняття (47 термінів), 2 – Види автоматизованих систем (25

термінів), 3 – Основні компоненти автоматизованих систем (27 термінів) тощо.

Стандартизовані терміни в стандарті надруковано напівжирним шрифтом, їхні короткі форми та абревіатури – світлим.

Наведені визначення можна за необхідності змінювати, вводячи до них похідні ознаки, розкриваючи значення використаних у них термінів, зазначаючи об'єкти, які входять у обсяг і зміст понять, визначених у цьому стандарті.

Терміни та визначення загальнотехнічних понять, необхідні для розуміння тексту стандарту, подано в додатку А.

У стандарті як довідкові подано англійські та російські еквіваленти стандартизованих термінів, а також визначення російською мовою, взяті з відповідних міжнародних і державних стандартів.

У стандарті наведено абеткові покажчики термінів та їхніх іншомовних еквівалентів.

Значення термінів та понять, наведених у стандарті, використовуються під час формування проєктів нормативно-правових актів та нормативних документів, які регламентують здійснення відповідних процесів експлуатації АС, а також забезпечення безпеки інформації, що в них обробляється (наприклад, у сфері технічного захисту інформації чинним є ***ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення"*** із встановленими термінами в цій сфері).

Із цією термінологією ми вже частково ознайомилися у Розділі 1 під час вивчення положень законодавчих та нормативно-правових актів, чинних у сфері ІБ держави.

Для прикладу наведу деякі з тих, що вживаються найчастіше:

система автоматизована (АС) – організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність;

інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

архітектура автоматизованої системи (далі – архітектура АС) – це концепція взаємозв'язку компонентів АС, що охоплює логічну, фізичну й програмну структури АС і принципи її функціонування;

захист – засіб обмеження доступу до використання всієї обчислювальної системи чи її частини;

адміністратор автоматизованої системи – особа (група осіб), яка здійснює координацію всіх робіт у процесі функціонування АС;

користувач інформації в системі (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі;

та інші терміни.

Отже, державний стандарт України 2226-93 "Автоматизовані системи. Терміни та визначення" встановлює терміни та визначення основних термінів та понять, які використовуються в різних сферах діяльності установ, метою яких є обробка інформації з використанням інформаційних (автоматизованих) систем. Встановлена стандартом термінологія надає можливість формулювати вимоги чинних НПА в сфері ІБ, що забезпечує єдине правильне розуміння суті викладених вимог усіма суб'єктами інформаційних відносин.

Розуміння суті термінів та понять дозволяє зрозуміти технології захисту інформації, які визначені в положеннях наступної низки НПА, чинних в цьому секторі ІБ.

2.1.2 "Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах" (постанова КМУ від 29 березня 2006 року № 373), зі змінами

Даний НПА визначає загальні *вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом***,** в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах установ; надає розширене розуміння правил забезпечення захисту інформації, яка в них обробляється.

Дія Правил не поширюється на захист інформації в *системах урядового та спеціальних видів зв'язку, в технічних засобах і їх складових, необхідних для здійснення уповноваженими органами оперативно-розшукових, розвідувальних заходів та негласних слідчих (розшукових) дій (захист інформації в таких системах та технічних засобах регламентуються іншими НПА та нормативними документами, призначення та головні положення яких розглядаються у розділі 3 цього посібника).*

Докладно розглянемо положення "Правил забезпечення захисту

інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах" (постанова КМУ від 29 березня 2006 року № 373). [32]

п. 4. Захисту в ІКС підлягає:

відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається електронними комунікаційними мережами (далі – відкрита інформація);

конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації" (далі – конфіденційна інформація);

службова інформація;

інформація, яка становить державну або іншу передбачену законом таємницю (далі – таємна інформація);

інформація, вимога щодо захисту якої встановлена законом.

п. 5. ***Відкрита інформація*** під час обробки в системі повинна *зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій,* які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. *Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження*.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, не ідентифікованими користувачами або користувачами з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора *повинні блокуватися*.

Створення та/або обробка в системі електронних документів, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, мають здійснюватися із застосуванням *кваліфікованого електронного підпису чи печатки*.

Перевірка та підтвердження кваліфікованого електронного підпису чи печатки здійснюються відповідно до вимог статті 18 Закону України "Про електронні довірчі послуги"

п. 6. ***Під час обробки службової і таємної інформації*** повинен забезпечуватися її *захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення*.

Доступ до службової інформації надається тільки *ідентифікованим та автентифікованим користувачам*.

Спроби доступу до такої інформації не ідентифікованих осіб чи користувачів з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора *повинні блокуватися*.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

п. 8. Вимоги до захисту в системі інформації, ***що становить державну таємницю, визначаються цими Правилами та законодавством у сфері охорони державної таємниці.***

Забезпечення технічного та криптографічного захисту інформації з обмеженим доступом, а також відкритої інформації, вимога щодо захисту якої встановлена законом, здійснюється в системі з дотриманням вимог, що висуваються для забезпечення захисту такої інформації, якщо інше не передбачене законом.

Криптографічний захист в системі таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, здійснюється з використанням засобів криптографічного захисту інформації, які відповідають вимогам до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації, що підтверджуються експертним висновком у сфері криптографічного захисту інформації або документом про відповідність.

Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються розпорядником інформації, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

У системі *здійснюється обов'язкова реєстрація*:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

спроб несанкціонованих дій з інформацією;

фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління

засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, і службовою інформацією повинна супроводжуватися повідомленням про них адміністратору безпеки (відповідальній особі).

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Автентифікація користувачів у системі здійснюється відповідно до вимог статті 17 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” та інших нормативно-правових актів.

Передача *конфіденційної інформації, службової та таємної інформації через незахищене середовище* (середовище, в якому циркулює інформація, стосовно якої відсутнє підтвердження відповідності захисту від усіх можливих загроз, імовірність прояву яких існує у цьому середовищі) здійснюється *у зашифрованому вигляді або захищеними каналами зв’язку згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації,* за винятком інформації, що передається через канали (лінії) зв’язку, які перебувають в межах контрольованої зони (територія (простір), на якій (в якому) унеможливлено несанкціоноване і неконтрольоване перебування сторонніх осіб, розміщення технічних і транспортних засобів).

Підключення систем, у яких обробляється службова інформація та інформація, що становить державну таємницю, до глобальних мереж передачі даних здійснюється з використанням *засобів криптографічного захисту інформації, які допущені до експлуатації для криптографічного захисту інформації відповідного ступеня обмеження доступу, та/або апаратних, апаратно-програмних засобів технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації та реалізують функції безпеки односпрямованої (односторонньої) передачі даних та/або двоспрямованої передачі даних з урахуванням їх змістовного аналізу*.

В апаратно-програмних засобах технічного захисту інформації, які реалізують функції односпрямованої (односторонньої) передачі даних та/або міжмережевого екранування (фільтрації) даних, що забезпечують захист службової інформації та інформації, що становить державну

таємницю, *рівень гарантії коректності надання функціональних послуг безпеки повинен бути не нижче третього*.

Достатність упроваджених засобів захисту інформації обґрунтовується на етапі технічного проєктування системи захисту інформації та оцінюється під час проведення державної експертизи комплексної системи захисту інформації.

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їхньої цілісності обробка в системі інформації припиняється.

Організаційні засади забезпечення захисту інформації

Для забезпечення захисту інформації в системі ***створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:***

витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації ***від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.***

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації.

Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування

комплексної системи захисту інформації. Умови, за яких можна не застосовувати комплексну систему захисту інформації, визначені Законом України “Про захист інформації в інформаційно-комунікаційних системах”.

У таких системах повинні бути виконані технічні та організаційні вимоги із захисту інформації, визначені цими Правилами.

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проєктування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

Якщо обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

План захисту інформації в системі містить:

завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

визначення моделі загроз для інформації в системі;

основні вимоги щодо захисту інформації та правила доступу до неї в системі;

перелік документів, згідно з якими здійснюється захист інформації в системі;

перелік і строки виконання робіт службою захисту інформації.

Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі – Адміністрація).

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.

У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проєктування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.

Порядок проведення державної експертизи системи захисту, державної експертизи засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.

Органи виконавчої влади, військові формування, створені відповідно до закону, які мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб, мають право організовувати проведення державної експертизи систем захисту на підприємствах, в установах, організаціях, закладах, військових з'єднаннях та частинах, які належать до їх сфери управління або підпорядковані їм. Порядок проведення такої експертизи встановлюється органом виконавчої влади, військовим формуванням, створеним відповідно до закону, за погодженням з Адміністрацією.

Контроль за забезпеченням захисту інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку, визначеному Адміністрацією.

У системі, яка складається з кількох інформаційних та (або) електронних комунікаційних систем, ці Правила можуть застосовуватися до кожної складової частини окремо.

Отже, "Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (постанова КМУ від 29 березня 2006 року № 373) (зі змінами), встановлюють загальні вимоги до системи забезпечення безпеки державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, під час їх обробки в інформаційних та інформаційно-комунікаційних системах установ.

Практичне впровадження встановлених *Правилами* вимог потребує більш детального їх формулювання, що і зроблено у цілій низці нормативних документів, які складають широкий перелік НД ТЗІ (нормативних документів у сфері технічного захисту інформації). Цей перелік нараховує десятки нормативних документів.

Розглянемо окремі із них, які містять ключові положення для розуміння принципів побудови системи безпеки інформації в установах, створення та впровадження комплексної системи захисту інформації в ІКС, обґрунтованої достатності комплексу засобів захисту в її складі, та інших важливих питань впровадження системи безпеки інформації.

2.1.3 “Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці” (НД ТЗІ 3.6-004-21)

Цей нормативний документ (НД) визначає ***основи організації та порядок впровадження системи безпеки інформації (СБІ) в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.***

НД ТЗІ 3.6-004-21 *визначає загальну систему дій щодо проєктування, впровадження, підтримки та постійного вдосконалення СБІ як частини загальної системи управління організацією, яка ґрунтується на підході управління ризиками безпеки та яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення безпеки інформації у поєднанні зі стратегічними, оперативними та бюджетними процесами планування в організації відповідно до міжнародних стандартів системи менеджменту інформаційної безпеки.* [33]

Вимоги НД розповсюджуються на інформаційні, інформаційно-комунікаційні, електронні комунікаційні системи, що розгорнуті та експлуатуються державними органами та установами, органами місцевого самоврядування, а також на підприємствах та організаціях всіх форм власності (далі – Організації).

Організаціям приватного сектору рекомендовано розглянути можливість використання цього нормативного документа залежно від обставин.

НД ТЗІ 3.6-004-21 *призначений для посадових осіб, пов'язаних з розробкою, розвитком, впровадженням, оцінкою, експлуатацією, обслуговуванням та розпорядженням Системи*, включаючи:

- суб’єктів інформаційних відносин (власників або розпорядників інформаційної системи, користувачів ІС), діяльність яких пов’язана з обробкою інформації, що підлягає захисту;
- осіб, діяльність яких пов’язана з використанням ІС в Організації, забезпеченням безпеки інформації, наглядом або управлінням (наприклад, керівники процесу управління ризиками, уповноважені посадові особи, співробітники підрозділів, що експлуатують інформаційну систему, адміністратори безпеки, співробітників служб захисту інформації та аналогічних підрозділів, відповідальні за безпеку інформації та приватність тощо);

– осіб, відповідальних за розробку та проєктування систем безпеки інформації, які можуть залучатися власником (розпорядником ІС) на договірних умовах;

– постачальників послуг безпеки та засобів захисту;

– осіб, відповідальних за проведення оцінювання впроваджених заходів захисту;

– осіб, відповідальних за проведення державної авторизації інформаційних систем.

Цей нормативний документ може бути застосований для захисту відкритої інформації, яка міститься в інформаційних системах, для забезпечення її цілісності та доступності.

Нормативний документ може застосовується для вибору та реалізації заходів захисту в інформаційних системах, спрямованих на забезпечення:

конфіденційності інформації (виключення неавторизованого доступу, копіювання, надання та розповсюдження);

цілісності інформації (виключення неавторизованого знищення та модифікації);

доступності інформації (виключення неавторизованого блокування інформації та інформаційної системи).

Досягнення належного рівня безпеки в організації вимагає:

чітко визначених та чітко сформульованих вимог безпеки та приватності для інформаційних систем і організацій;

суворого планування безпеки та приватності, а також управління життєвим циклом інформаційної системи й інформації;

використання надійних компонентів інформаційної системи, сучасних апаратних засобів і програмного забезпечення для захисту інформації;

застосування системного підходу до забезпечення безпеки та приватності;

ефективного процесу інтеграції засобів захисту в інформаційні системи;

застосування добре задокументованих та інтегрованих у процеси практик безпеки та приватності;

постійного моніторингу інформаційних систем і організацій для визначення поточного стану ефективності заходів захисту, необхідних змін в інформаційних системах і робочих середовищах, а також стану безпеки та приватності в цілому.

Розглянемо положення цього НД ТЗІ. [32]

Організації мають проводити аналіз і реально оцінювати ризики безпеки для своїх операцій (процесів) і активів, фізичних осіб, інших організацій і держави, які виникають в результаті виконання їхніх завдань і функцій (процесів). Реалістичне оцінювання ризиків безпеки потребує глибокого розуміння загроз безпеки, реалізація яких ґрунтується на вразливостях інформаційних систем і організації в цілому, імовірності та можливих негативних наслідків, що виникають у разі порушення конфіденційності, цілісності, доступності та інших властивостей безпеки. Оцінювання ризиків безпеки також потребує розуміння ризиків приватності. Вимоги безпеки та приватності повинні бути сформульовані з урахуванням стратегії управління ризиками організації з увагою на особливості, витрати, порядок і ефективність впровадження заходів, пов'язаних з проєктуванням, розробкою, придбанням, розгортанням, експлуатацією та підтримкою інформаційних систем організації.

Результати оцінювань ризиків мають бути джерелом інформації для процесу вибору заходів захисту.

Процес вибору призводить до формування узгодженого ***набору заходів захисту – профілю безпеки, що відповідає конкретним потребам організації***. Цей процес має бути гнучким для того, щоб організації могли ефективно пристосовуватися до складних і мінливих умов функціонування інформаційних систем та робочого середовища.

Модель порядку впровадження СБІ

Впроваджені ***системи безпеки інформації (СБІ)*** мають забезпечувати задоволення вимог щодо захисту інформації. Такі вимоги можуть бути сформульовані національними та міжнародними інстанціями. *Необхідною умовою забезпечення інтероперабельності національних систем з міжнародними партнерами є можливість легкого впровадження міжнародних стандартів у галузі безпеки інформації FIPS PUB 199, FIPS PUB 200, NIST Special Publication 800-30, NIST Special Publication 800-37, NIST Special Publication 800-39, NIST Special Publication 800-53, NIST Special Publication 800-64, NIST Special Publication 800-128, NIST Special Publication 800-160. Для більш швидкого та ефективного розроблення СБІ необхідним вбачається впровадження механізму, який здатен забезпечити легкий процес інтеграції галузевих національних та міжнародних стандартів безпеки.*

При побудові СБІ має бути забезпечена можливість «персоналізації» даного процесу для кожної ІС. Під персоналізацією мається на увазі можливість гнучкого процесу проєктування системи безпеки інформації,

яка максимально забезпечує задоволення потреб конкретної ІС та є економічно ефективною.

Рішення щодо типу СБІ для розгортання в конкретній ІС має ухвалюватися залежно від типу ІС та інформації, яка в ній циркулює. В рамках даного НД для визначення типу інформації використовується наступна класифікація інформації за типом властивостей, що забезпечуються (рисунок 5.1) *(нумерація рисунку надається відповідно до НД ТЗІ).*



Рисунок 5.1. Класифікація інформації за типом властивостей, що забезпечуються

Для рішення щодо типу СБІ, яка розгортається в ІС, використовують таку модель (таблиця 5.1) *(нумерація таблиці надається відповідно до НД ТЗІ).*

Власники інформаційних систем, які обробляють ***відкриту інформацію*** не залежно від форми власності ІС, *мають розгортати системи безпеки інформації (СБІ), керуючись положеннями цього нормативного документу для впровадження відповідних заходів захисту, направлених на забезпечення цілісності та доступності відкритої інформації, яка циркулює у даних ІС.*

Власники ІС, які обробляють будь-які ***персональні дані*** (далі – ПД), не залежно від форми власності ІС, мають розгортати СБІ, керуючись положеннями цього нормативного документа, а також вимог національного стандарту ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)» для впровадження відповідних заходів захисту, направлених *на забезпечення конфіденційності, цілісності та доступності ПД*. Власники ІС, які обробляють ПД та знаходяться у приватній власності, додатково можуть ухвалити рішення щодо впровадження відповідності ІС вимогам міжнародних Регламентів (GDPR).

Державні ІС, в яких циркулює ***критична інформація****, мають розгортати СБІ, керуючись положеннями цього нормативного документа для впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності критичної інформації, яка циркулює у таких ІС.*

Критична інформація розрізняється за рівнем критичності: ***низький, середній, високий.*** До критичної інформації також належать: *комерційна таємниця, банківська таємниця, таємниця слідства, службова інформація тощо*.

ІС, які відповідно до Постанови Кабінету Міністрів України № 943 від 09.10.2020 р. та Постанови Кабінету Міністрів України № 1109 від 09.10.2020 р., розгортаються на ОКІІ І-ІІ категорії критичності, мають розгортати СБІ, керуючись положеннями цього нормативного документа для *впровадження відповідних заходів захисту, направлених на забезпечення конфіденційності, цілісності та доступності критичної інформації, яка циркулює у таких ІС.* ІС, які відповідно до Постанови Кабінету Міністрів України № 943 від 09.10.2020 р. та Постанови Кабінету Міністрів України № 1109 від 09.10.2020 р., розгортаються на ОКІІ ІІІ - IV категорії критичності, можуть розгортати СБІ, керуючись положеннями цього нормативного документа або міжнародних стандартів, враховуючи особливості ІС та умови її функціонування. Незалежно від категорії критичності об’єкти критичної інфраструктури, в інформаційних системах, у яких циркулює критична інформація, мають проходити процедуру державної авторизації розгорнутої СБІ.

ІС, у яких циркулює ***секретна інформація, мають розгортати комплексну систему захисту інформації (КСЗІ)****, керуючись вимогами чинного національного законодавства.*

Таблиця 5.1 – Модель впровадження системи безпеки інформації

<table>
<tr><td colspan="3" rowspan="3">Типи інформації
Типи ІС</td><td colspan="6">Інформація з обмеженим доступом</td><td rowspan="3">Відкрита інформація</td></tr>
<tr><td colspan="3">Секретна</td><td colspan="3">Критична інформація</td><td rowspan="2">Персональні дані</td></tr>
<tr><td colspan="3">Гриф секретності</td><td colspan="3">Рівень критичності</td></tr>
<tr><td colspan="2"></td><td>Т</td><td>ЦТ</td><td>ОВ</td><td>Високий</td><td>Середній</td><td>Низький</td><td></td><td></td></tr>
<tr><td colspan="2">Державні ІС</td><td colspan="3">Комплексні системи захисту інформації (КСЗІ)</td><td colspan="3">СБІ відповідно до національних вимог
+ державна авторизація</td><td>СБІ відповідно до національних вимог
Додаткові вимоги ДСТУ 7731:2015</td><td>СБІ</td></tr>
<tr><td rowspan="2">ОКІІ</td><td>І/ІІ категорія критичності</td><td colspan="3" rowspan="2">КСЗІ</td><td colspan="3">СБІ відповідно до національних вимог
+ державна авторизація</td><td rowspan="2">СБІ відповідно до національних вимог
Додаткові вимоги ДСТУ 7731:2015</td><td rowspan="2">СБІ</td></tr>
<tr><td>ІІІ/IV категорія критичності</td><td colspan="3">СБІ відповідно до національних /міжнародних вимог
+ державна авторизація</td></tr>
<tr><td colspan="2">ІС у приватній власності</td><td colspan="3">КСЗІ</td><td colspan="3">СБІ відповідно до національних/міжнародних вимог</td><td>СБІ відповідно до національних вимог
Додаткові вимоги ДСТУ 7731:2015 / GDPR</td><td>СБІ</td></tr>
<tr><td colspan="2" rowspan="2">Класифікація ІС</td><td colspan="3" rowspan="2">Відповідно до НД ТЗІ 2.5-005 -99
АС клас 1
АС клас 2
АС клас 3</td><td colspan="3">Відповідно до НД ТЗІ 3.6-004-21</td><td rowspan="2">-</td><td rowspan="2">-</td></tr>
<tr><td>ІС з високою категорією критичності</td><td>ІС з середньою категорією критичності</td><td>ІС з низькою категорією критичності</td></tr>
</table>

Забезпечення взаємодії між рівнями системи безпеки інформації Організації.

Система безпеки інформації – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки в Організації.

СБІ повинна забезпечити безпечність та надійність виконання функцій/процесів за призначенням Організації. Впровадження та функціонування СБІ стосується всіх підрозділів Організації. Тому відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їхньої відповідальності, під час впровадження та функціонування СБІ.

Цілі СБІ, заходи захисту (наявні або ті, що будуть впроваджені), документація, що описує функціонування СБІ, повинні бути зрозумілими для всіх зацікавлених сторін (стейкхолдерів).

Впровадження в Організації СБІ дозволить:

- оптимізувати вартість побудови та підтримання системи інформаційної безпеки;
- постійно відслідковувати та оцінювати ризики безпеки з урахуванням призначення (місії) Організації (цілей бізнесу);
- ефективно виявляти ризики безпеки та знижати ймовірність їх виникнення;
- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;
- ефективно розробляти, впроваджувати та тестувати заходи захисту інформації;
- забезпечити розуміння питань інформаційної безпеки та приватності керівництвом та всіма працівниками Організації.

Управління ризиками безпеки та приватності вимагає участі посадових осіб на всіх ланках управління Організації – від керівництва, що визначає стратегічне бачення (місію), цілі та задачі для Організації, до керівників середньої ланки, які здійснюють планування, виконання та управління функціями/процесами, та осіб, які розробляють, впроваджують, використовують і підтримують системи та процеси управління ризиками. Такий підхід підтримує виконання функціональних завдань Організації та реалізації процесів. Управління ризиками є цілісною діяльністю, яка впливає на всі аспекти діяльності Організації, включаючи планування, архітектуру підприємства, процеси життєвого циклу розробки системи (system development life cycle – SDLC).

На рисунку 6.1 наведено багаторівневий підхід до управління ризиками безпеки та приватності. Управління ризиками здійснюється на

організаційному, процесуальному (функціональному) та на системному рівнях.

Взаємодія між рівнями забезпечується двоспрямованими інформаційними потоками. Це дозволяє обробляти ризики безпеки на всіх рівнях.

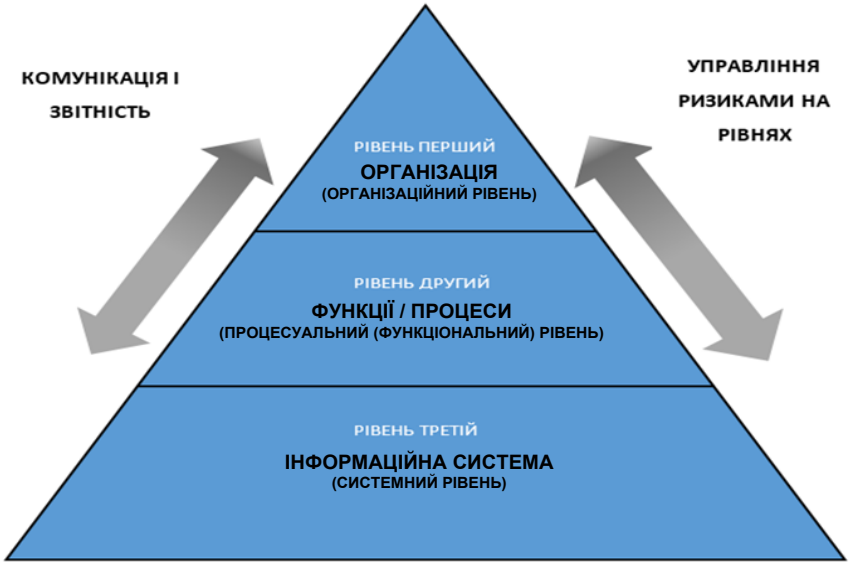


Рисунок 6.1. Загальний підхід щодо управління ризиками безпеки

Типи заходів захисту та особливості їхнього застосування

Заходи, що проводяться на організаційному, процесуальному (функціональному) та системному рівнях (рисунок 6.2) є важливими для підготовки Організації до реалізації концепції управління ризиками та впровадження СБІ. Така підготовка передбачає широкий спектр заходів.

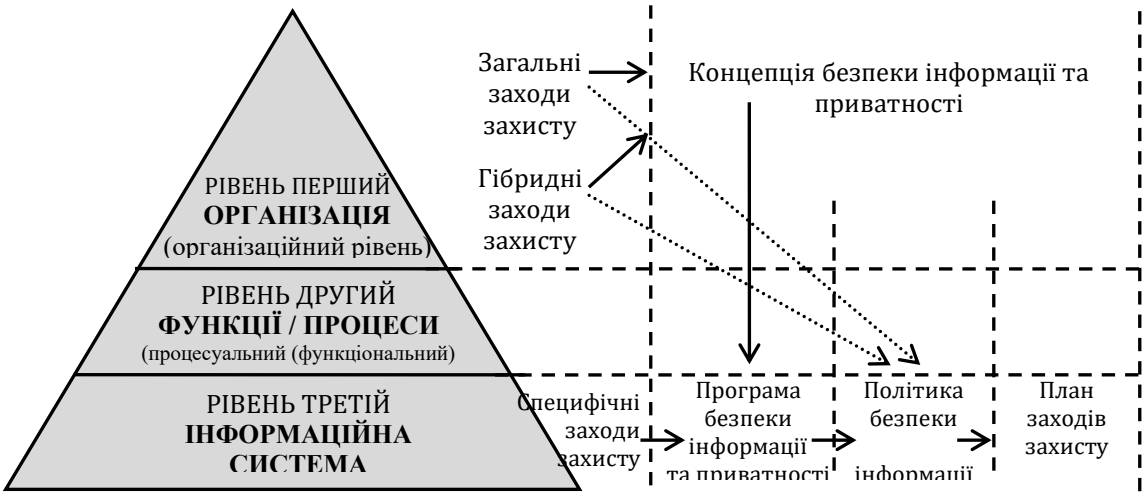


Рисунок 6.2. Розподіл заходів захисту за рівнями управління ризиками в організації

Ухвалення рішення щодо управління ризиками безпеки на системному рівні тісно пов’язане з такими аспектами:

- призначення (місія, цілі), завдання, функції та процеси Організації;
- ініціативи з модернізації ІС, компонентів та послуг ІС;
- архітектура підприємства, зменшення складності ІС шляхом інтеграції, оптимізації та стандартизації;
- розподіл ресурсів для забезпечення ефективного, результативного та економічно-вигідного виконання функцій/ процесів та досягнення цілей Організації.

НД ТЗІ 3.6-004-21 визначає три типи заходів захисту інформації та персональних даних:

загальні заходи захисту;

специфічні для інформаційної системи заходи захисту (далі – *специфічні заходи захисту*);

гібридні заходи захисту.

Тип заходу захисту визначає:

- сферу застосування заходу захисту;
- спільний характер або спадковість заходів захисту;
- відповідальність за розробку (налаштування), впровадження, оцінювання та надання дозволу на впровадження заходу захисту.

Кожен тип заходу захисту має конкретну спрямованість і завдання, що допомагає організаціям ефективно впроваджувати його та отримувати очікувані результати в контексті виконання вимог безпеки. Застосування певних типів заходів захисту забезпечує оптимізацію витрат (часових, матеріальних, людських) у різних інформаційних системах і робочих середовищах на впровадження (реалізацію) заходів захисту та побудову системи захисту інформації в цілому.

Загальні заходи захисту.

Загальні заходи захисту можуть бути використані для декількох інформаційних систем одночасно. Захід захисту вважається *успадкованим*, коли інформаційна система використовує результати захисту від впровадженого заходу захисту, що контролюється, впроваджується (реалізується), оцінюється, санкціонується суб’єктами, які не несуть відповідальності за цю інформаційну систему.

Загальні заходи захисту можуть впроваджуватися різними технологіями: застосування засобів захисту периметру, засобів управління доступом, засобів ідентифікації та автентифікації, а також заходів захисту,

які є елементом міждоменних рішень. Витрати на розробку, впровадження (реалізацію), оцінювання, акредитацію та моніторинг загальних заходів захисту можуть бути амортизовані в різних інформаційних системах і організаційних елементах.

Вибір загальних заходів захисту рекомендовано здійснювати на загальноорганізаційній основі із залученням керівництва організації, яке розуміє цілі та завдання організації, організаційні ризики безпеки, важливість інформаційних систем, що підтримують функції, процеси та активи організації. Залучення керівництва організації забезпечить оптимальність розподілу ресурсів і відповідальності щодо розроблення, впровадження, оцінювання, надання дозволу та моніторингу загальних заходів захисту.

Відповідальність за провадження загальних заходів захисту покладається на конкретних посадових осіб. Ці посадові особи розробляють, впроваджують, оцінюють, акредитують і контролюють вибрані організацією для впровадження (реалізації) загальні заходи захисту.

Визначення та вибір загальних заходів захисту найефективніше проводити в співпраці з уповноваженими посадовими особами, представниками керівництва, власниками бізнесу, аналітиками безпеки, власниками (розпорядниками) інформації та з іншими зацікавленими сторонами.

Загальні заходи захисту мають бути задокументовані в програмі (концепції) безпеки інформації та приватності організації. Вони також можуть бути задокументовані в політиках безпеки інформаційних систем, які успадковують ці заходи захисту, або в ситуаціях, коли загальні заходи захисту впроваджуються в межах конкретних інформаційних систем. Загальні заходи захисту можуть бути описані в одному документі або в кількох документах з посиланнями на інші документи. Якщо програма (концепція) безпеки інформації та приватності складається з декількох документів, у кожному документі мають бути визначені посадові особи, відповідальні за розробку, реалізацію, оцінювання, акредитацію та моніторинг відповідних загальних заходів захисту. Якщо загальні заходи захисту вносяться в окрему політику безпеки інформаційної системи, концепція безпеки інформації та приватності організації має вказувати, які окремі політики безпеки містять опис загальних заходів захисту.

Заходи захисту, які не визначені як загальні заходи, вважаються *специфічними або гібридними*. За впровадження специфічного заходу захисту, що стосується конкретної інформаційної системи, відповідальність несуть власники (розпорядники) та посадові особи цієї інформаційної системи.

Захід захисту може бути визначений *як гібридний*, якщо одна частина заходу захисту є загальною, а інша частина заходу захисту є специфічною для інформаційної системи. Наприклад, організація може реалізовувати заходи планування безперервної роботи, використовуючи для всіх інформаційних систем заздалегідь погоджений з окремими власниками (розпорядниками) шаблон плану, пристосовуючи план для конкретного використання. Розподіл гібридних заходів захисту на загальні та специфічні може залежати від організації, типів використовуваних інформаційних технологій, розподілу обов'язків і методів (механізмів), що використовуються організацією для реалізації заходів захисту.

Визначення того, чи є захід захисту загальним, гібридним або специфічним, залежить від контексту його впровадження (реалізації). Захід захисту не можна визначити загальним, гібридним або специфічним, лише ґрунтуючись на його формулюванні. Наприклад, захід захисту може бути специфічним для однієї інформаційної системи, і водночас може бути загальним заходом для іншої інформаційної системи (тобто успадкованим від першої системи). Одним з методів визначення того, чи може специфічний захід бути загальним заходом для інших інформаційних систем, є розгляд того, хто чи що залежить від функціональності цього заходу захисту. Якщо певна частина інформаційної системи, що є зовнішньою для цієї системи, залежить від заходу захисту, то цей захід може бути загальним.

Розмежування заходів захисту на загальні, гібридні та специфічні може допомогти оптимізувати витрати на впровадження та оцінювання заходів захисту, а також забезпечити гнучкість і послідовність застосування засобів захисту в рамках всієї організації. Хоча розподіл заходів захисту на загальні, гібридні й специфічні є простим та інтуїтивно зрозумілим, фактично застосування зазначених заходів вимагає планування та координації діяльності із захисту інформації.

Документування заходів захисту

До основних документів, які мають бути сформовані та затверджені в Організації на ІС належать наступні:

- *концепція безпеки інформації та приватності;*
- *опис ІС;*
- *категорія критичності;*
- *програма безпеки інформації та приватності;*
- *політики безпеки інформації;*
- *плани заходів захисту інформації та персональних даних.*

Даний перелік не є вичерпним і може доповнюватися на розсуд Власника (Розпорядника) Організації та/або ІС виходячи із особливостей Організації/ІС та/або нормативних вимог, сформованих центральними або галузевими органами влади.

Етапи розгортання системи безпеки інформації

Розгортання та подальше функціонування СБІ здійснюється як безперервна цілеспрямована діяльність Організації, яка складається з етапів та завдань (рисунок 6.3).

Організації під час впровадження СБІ слід дотримуватися послідовного підходу, який застосовується до всіх етапів управління ризиками в масштабах всієї організації: від організаційного до системного рівня. Відповідальні особи Організації визначають та захищають необхідні ресурси для виконання завдань щодо управління ризиками та забезпечують доступність цих ресурсів для відповідного персоналу.

Діяльність з впровадження СБІ складається ***з семі етапів***:

- ***аналіз ризиків на організаційному та системному рівнях;***
- ***категоріювання безпеки;***
- ***вибір заходів захисту;***
- ***впровадження заходів захисту;***
- ***оцінювання безпеки;***
- ***авторизація безпеки ІС;***
- ***постійний моніторинг безпеки.***

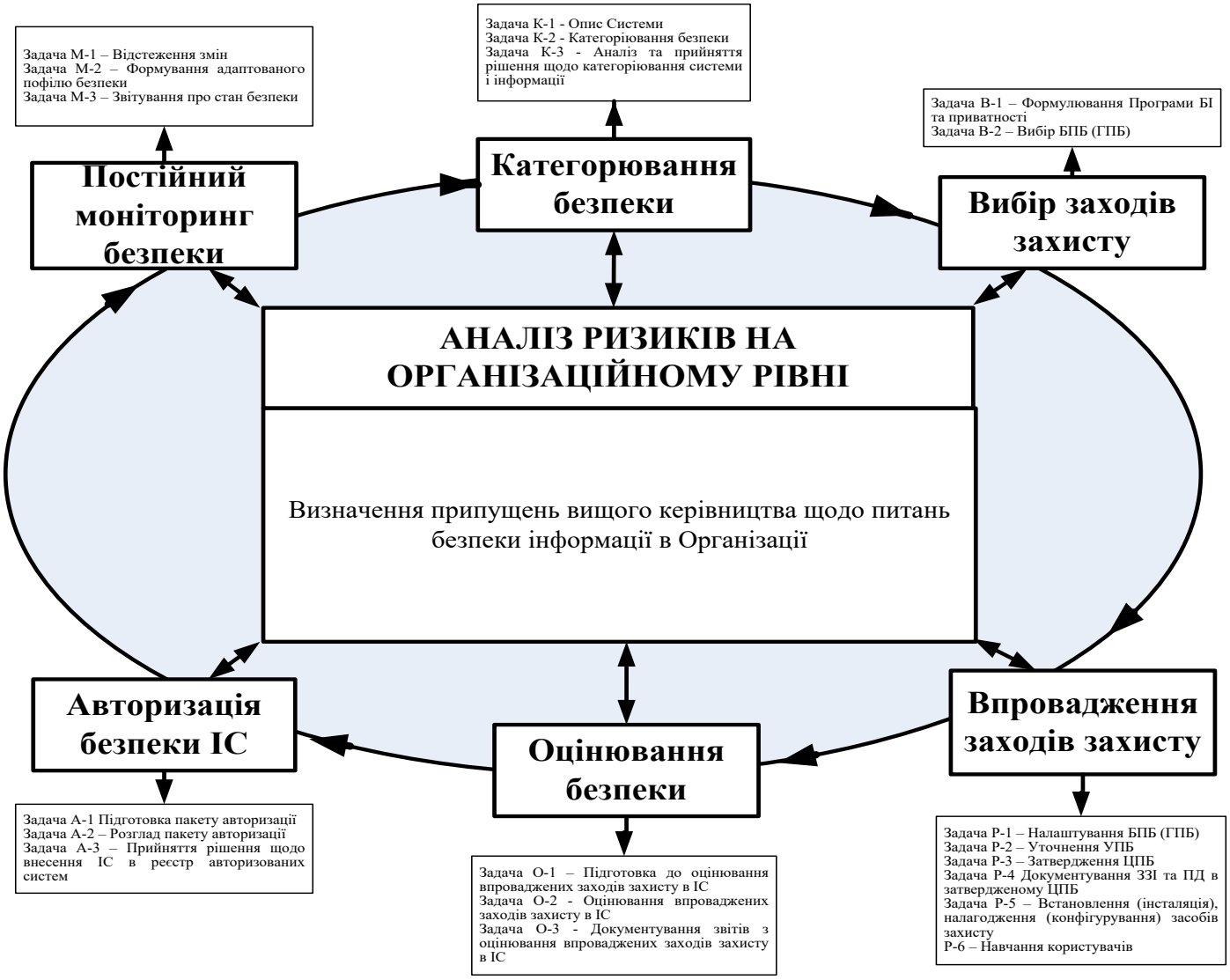


Рисунок 6.3 – Етапи впровадження системи безпеки інформації в Організації

Усі виконані дії щодо виконання вище зазначених етапів повинні документуватися відповідальними особами в частині, яка регулюється їхніми повноваженнями. За своїми ролями та впливом при виконанні на процесів аналізу ризиків на організаційному рівні, категоріювання безпеки, вибір, впровадження та оцінювання безпеки, а також авторизації безпеки ІС та процесів постійного моніторингу безпеки, усі особи можливо розподілити на наступні:

1. Власник ІС (Розпорядник).
2. Розробник (Проєктувальник) системи захисту інформації. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як проєктувальник системи безпеки, проєктувальник системи приватності. За необхідності для виконання цієї ролі можуть залучатися сторонні фахівці на договірній основі.
3. Постачальник послуг безпеки та засобів захисту. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як інженер з безпеки системи, інженер з приватності системи. За необхідності для виконання цієї ролі можуть залучатися сторонні фахівці на договірній основі.
4. Адміністратор безпеки. Ця роль може поєднувати функціональні обов'язки таких посадових осіб, як службова особа з безпеки, службова особа з приватності, системний адміністратор.
5. Оцінювач безпеки/група оцінювачів. Для виконання цієї ролі повинні залучатися сторонні фахівці на договірній основі.
6. Уповноважений орган з авторизації.

В свою чергу, кожній з етапів складається із завдань. Кожне завдання розглядається як функціональний блок, який містить мету, вхідні дані, вихідні дані та перелік ролей, що відповідають за виконання завдання.

Впровадження вимог цього та інших НД з питань управління безпекою інформації є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи безпеки інформації (СБІ).

Цей нормативний документ щодо впровадження системи безпеки інформації деталізує вимоги міжнародного стандарту ISO/IEC 27003:2010 "Information technology – Security techniques – Information security management system implementation guidance" (Настанова з упровадження системи управління інформаційною безпекою) з урахуванням особливостей діяльності організацій, установ, відомств та підприємств з питань безпеки інформації. Модель, що впроваджується цим НД, конкретизує модель ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2015 *(Ця відповідність наочно проілюстрована на рисунку 6.4 НД ТЗІ)*.

Відповідність СБІ, закріпленої в цьому нормативному документі, вимогам міжнародних стандартів ISO/IEC 27001 та ISO/IEC 27002 надасть можливість власниками ІС, які розгорнули СБІ керуючись положеннями

цього НД за потреби також *отримати відповідний міжнародний сертифікат.*

Кожний з етапів має перелік вхідних та вихідних даних. Вихідні дані кожного з етапів можуть бути вхідними для подальших.

Впровадження заходів захисту як життєвий цикл розробки IT-систем

З метою підвищення ефективності системи безпеки інформації, вона має бути інтегрована до життєвого циклу розробки IT-систем (SDLC) з самого початку створення систем.

Є багато методологій SDLC, які можуть використовуватися організацією, щоб ефективно розробити інформаційну систему. Традиційний SDLC – лінійна послідовна модель (також відома як метод водоспаду), передбачає, що система буде поставлена в її заключних етапах життєвого циклу розробки. Інший метод SDLC використовує модель прототипування, яка часто застосовується, щоб зробити можливим розуміння системних вимог, не розробляючи насправді закінчену інформаційну систему. Складніші системи можуть зажадати моделей більш ітераційної розробки. Так, складні моделі розроблялися та успішно використовувалися, щоб врахувати розвинуту складність передових та іноді великих проєктів інформаційних систем. Прикладами таких складних моделей є:

модель швидкої розробки додатків (RAD);
модель спільної розробки додатків (JAD);
модель прототипування;
спіральна модель.

Очікуваний розмір і складність системи, графік розробки та тривалість життя системи будуть впливати на вибір того, яку модель SDLC використовують. В багатьох випадках вибір моделі SDLC буде визначений Концепцією безпеки інформації Організації.

Типовий SDLC включає п'ять фаз (рисунок 7.1):
ініціювання;
розробка / придбання;
реалізація / оцінка;
експлуатація / підтримка;
ліквідація.

Кожна фаза включає мінімальний набір завдань з безпеки інформації, необхідних для ефективного включення безпеки в процес розробки системи. Фази можуть постійно повторюватися протягом життя системи до

виведення її з експлуатації.

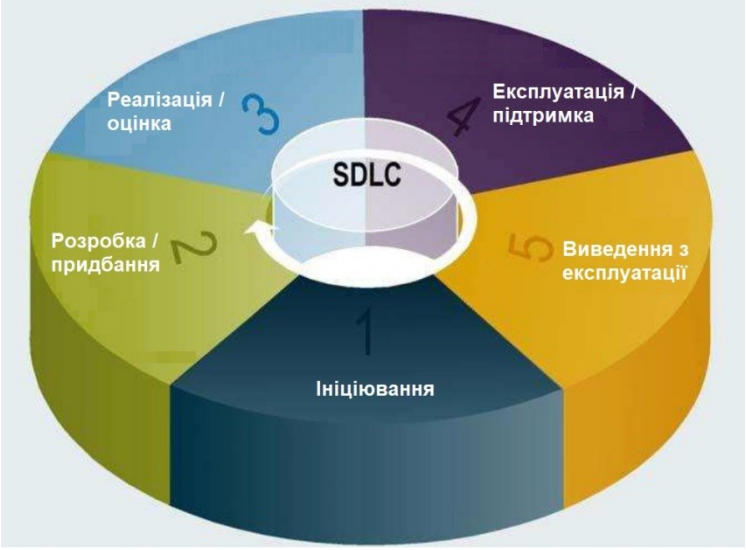


Рисунок 7.1. Концептуальне подання SDLC

Ініціювання. Під час фази ініціювання виражається потреба в системі та документується призначення системи. Під час цієї першої фази життєвого циклу розробки розгляд безпеки є ключовими для ретельної та ранньої інтеграції, гарантуючи, таким чином, що будуть розглянуті загрози, вимоги та потенційні обмеження у функціональності та інтеграції. У цей момент на безпеку дивляться більше з точки зору ризиків для діяльності з позиції служби інформаційної безпеки.

Розробка / придбання. Під час цієї фази система проєктується, закуповується, програмується, розробляється або інакше створюється. Ключові роботи з безпеки для цієї фази охоплюють:

проведення оцінки ризику та використання результатів для доповнення базового набору заходів забезпечення безпеки;

аналіз вимог безпеки;

проведення функціонального тестування та тестування безпеки;

підготовку вихідних документів до сертифікації та атестації системи;

проєктування архітектури безпеки.

Реалізація / оцінка. Під час цієї фази система повинна бути встановлена та оцінена в експлуатаційному середовищі Організації. Ключові роботи з безпеки для цієї фази включають:

інтеграцію інформаційної системи в її середовище;

планування та проведення робіт по оціночним випробуванням системи в синхронізації з тестуванням заходів безпеки;

роботи по комплексній оцінці системи.

Експлуатація / підтримка. Під час цієї фази система виконує свою

роботу. Система майже завжди змінюється з додаванням апаратного та програмного забезпечення та різними іншими подіями. У цій фазі системи розгорнуті та експлуатуються поліпшення та/або модифікації для систем розроблені й протестовані, й апаратні засоби та/або програмне забезпечення додані або замінені. Систему контролюють для тривалої роботи відповідно до вимог безпеки та впроваджують необхідні модифікації системи. Експлуатована система періодично оцінюється, щоб визначити, як система може бути зроблена більш ефективною, безпечною та результативною. Експлуатація триває до тих пір, поки система може бути ефективно змінена, щоб відповісти на потреби Організації, та підтримується на встановленому рівні ризику. Коли визначена необхідність модифікації або змін, система може повторно перейти в попередню фазу SDLC. Ключові роботи з безпеки для цієї фази включають:

проведення аналізу експлуатаційної готовності;

управління конфігурацією системи;

встановлення процесів і процедур для надійної експлуатації та безперервного моніторингу заходів безпеки інформаційної системи;

виконання повторного санкціонування за необхідності.

Виведення з експлуатації. Роботи, проведені під час цієї фази, гарантують організоване припинення функціонування системи, збереження суттєвої інформації системи, а переносяться дані, передаються системою до нової системи, або зберігаються відповідно до застосовних нормативних документів та політик управління записами. Проблеми безпеки інформації, пов'язані з ліквідацією інформації й системи, повинні бути повністю вирішені. Коли інформаційні системи передаються, стають застарілими або більше не застосовні, важливо гарантувати, що ресурси та активи захищені. Зазвичай, це не остаточний кінець системи. Системи зазвичай розвиваються або переходять до наступного покоління через зміни вимог або поліпшення технологій. Плани забезпечення безпеки системи повинні безперервно розвиватися з системою. Крім того, велика частина інформації щодо оточення, управління та експлуатації повинна бути відповідною і корисною в розробці плану забезпечення безпеки для системи.

Роботи по виведенню з експлуатації гарантують акуратне завершення використання системи та зберігають важливу інформацію про систему так, щоб деяка або вся інформація могла б бути, в разі необхідності, відновлена в майбутньому. Особливий акцент робиться на належному збереженні даних, які обробляються системою з тим, щоб дані були ефективно переміщені в іншу систему або заархівовані відповідно до застосовних нормативних актів та політик з управління записами для потенційного майбутнього доступу.

Роботи з розгортання системи безпеки повинні бути фізично й логічно інтегровані в політику й керівництво Організації по SDLC.

Визначення етапів розгортання системи безпеки інформації

1) етап аналізу ризиків на організаційному рівні

Цей етап передбачає підготовку на Організаційному рівні до реалізації процесів управління ризиками безпеки і включає:

визначення ролей в Організації в сфері управління ризиками безпеки;

розробку Концепції ІБ та приватності;

визначення цілей, завдань, функцій та процесів, які має підтримувати інформаційна системи (фокус ІС);

визначення ключових стейкхолдерів (внутрішніх і зовнішніх для організації), які зацікавлені у функціонуванні ІС;

розуміння загроз та потенційного негативного впливу загроз на фізичних осіб та інформаційні системи;

проведення оцінювання ризиків на рівні Організації;

визначення (вибір) та розстановку пріоритетів вимог безпеки та приватності;

визначення та узгодження вимог безпеки та приватності;

побудову ІС (сукупності ІС).

2) етап категоріювання безпеки

З метою оцінки рівня критичності активів Організації та ІС проводиться категоріювання всіх активів ІС на основі її опису. Категоріювання проводиться з точку зору оцінки рівня негативного впливу (шкоди), який може настати в разі, якщо будуть порушені конфіденційність, цілісність та доступність активів ІС. Для цього визначаються критерії оцінки впливу за кожною властивістю безпеки та встановлюється *рівень критичності – низький, середній та високий*. Порядок оцінки критичності та проведення категоріювання встановлюється окремим нормативним документом «Порядок категоріювання безпеки інформаційної системи та інформації».

3) етап вибору заходів захисту

Організація за результатами оцінки ризиків безпеки та категоріювання безпеки обирає набір заходів захисту – базовий (галузевий) профіль безпеки. Заходи захисту обираються на основі системи заходів захисту, що встановлюється окремим нормативним документом, спираючись на стандартні профілі безпеки та профілі кібербезпеки. Під час визначення заходів захисту також враховуються профілі безпеки засобів захисту,

вимоги міжнародних та галузевих стандартів. Порядок вибору базового (галузевого) профілю безпеки встановлюється окремим нормативним документом «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

4) етап впровадження (реалізації) заходів захисту

Впровадження (реалізація) заходів захисту здійснюється відповідно до розробленої Концепції безпеки інформації та приватності із застосуванням методології проєктування систем захисту інформації. Особливості впровадження заходів захисту визначаються окремим нормативним документом «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

5) етап оцінювання безпеки

Перевірка відповідності заходів захисту встановленим вимогам безпеки та приватності здійснюється під час оцінювання безпеки. Під оцінюванням мається на увазі широкий спектр підходів до встановлення коректності реалізації заходів захисту інформації та ПД в ІС відповідно до обраного профілю захисту. Порядок та методика визначаються окремим нормативним документом «Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

6) етап авторизації безпеки інформаційної системи

Рішення щодо можливості використання СБІ інформаційної системи набирає чинності в результаті внесення запису до реєстру авторизованих систем. Рішення ухвалюється уповноваженим органом з авторизації. Для проведення авторизації формується пакет відповідних документів (пакет авторизації), що подається до уповноваженого органу з авторизації. Порядок проведення державної авторизації встановлюється нормативним документом «Порядок авторизації безпеки інформаційних систем».

7) етап постійного моніторингу безпеки

Моніторинг безпеки є важливим етапом відстеження змін стану безпеки ІС та Організації та реагування на нові виклики (загрози) безпеки. З цією метою в Організації розробляється стратегія постійного моніторингу. Відповідний Порядок проведення встановлюється окремим нормативним документом «Порядок моніторингу безпеки інформаційних систем».

Отже, *НД ТЗІ 3.6-004-21 "Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці" визначає порядок організації та послідовність впровадження системи безпеки інформації (СБІ) в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. Система безпеки інформації різного ступеня критичності (на об'єктах відповідної категорії) повинна передбачати й відповідні переліки заходів та засобів захисту. Чим вищий рівень критичності оброблюваної в ІКС інформації, тим вищі вимоги щодо гарантій безпеки інформації, які повинні забезпечити впроваджені заходи та засоби захисту.*

В ІКС, в яких обробляється інформація, що складає державну таємницю, повинна бути ***створена комплексна система захисту інформації****.*

Важливими чинниками ухвалення правильних рішень щодо побудови системи захисту інформації в ІКС є приналежність їх до ***певної категорії та класу.***

Ці питання потребують детального вивчення.

2.1.4 Категорії об'єктів та інформаційних і інформаційно-комунікаційних систем (далі – ІС)

Для органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, органів судової влади, правоохоронних та інших державних органів, а також підприємств, установ, закладів і організацій незалежно від форми власності, на об'єктах яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, обов'язковими є вимоги ***категоріювання*** як самих об'єктів, так й інформаційних систем, які функціонують на них.

Під терміном ***"категоріювання"*** *мають на увазі* ***сукупність дій зі встановлення категорії об'єкта****.*

Категорія (об'єкта) *– класифікаційна характеристика важливості об'єкта, за якою визначається необхідний (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об'єкті.*

Категоріювання здійснюється з метою визначення необхідного ***рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті****.*

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи-власника (розпорядника, користувача) об'єкта.

Категоріювання здійснюється за такою ознакою: ***ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.***

Відповідно до цієї ознаки, об'єктам, на яких обробляється технічними засобами та/або озвучується ІзОД, може бути встановлена одна із наступних категорій (наведено від нижчої до найвищої категорії):

четверта (IV) категорія – у разі обробки на об'єкті службової інформації, яка має ступінь обмеження "для службового користування";

третя (III) категорія – у разі обробки на об'єкті інформації, яка має ступінь обмеження "таємно";

друга (II) та перша (I) категорії – у разі обробки на об'єкті інформації, яка має ступінь обмеження "цілком таємно" та "особливої важливості" і відповідно.

Об'єкти, яким встановлено відповідну категорію, вносяться до ***Переліку категорійованих об'єктів, який веде власник*** (розпорядник, користувач) об'єктів інформаційної діяльності.

Отже, положеннями нормативних документів системи технічного захисту інформації визначений порядок категоріювання об'єктів (зокрема й ІС). Категорія об'єкта (ІС) – це класифікаційна характеристика важливості об'єкта, за якою визначається необхідний рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об'єкті. Категорія об'єкта суттєво впливає на склад комплексу засобів захисту інформації та інших організаційно-технічних заходів, які необхідно впроваджувати на об'єктах інформаційної діяльності.

2.1.5 Встановлені класи та можливі стандартні функціональні профілі захищеності інформації в ІКС (НД ТЗІ 2.5-005-99)

Окрім ***категорії*** ОІД (ІКС) важливим чинником, який суттєво впливає на обсяг організаційно-технічних заходів забезпечення безпеки інформації на ОІД, ***є клас, до якого належить ІКС, і можливий стандартний функціональний профіль захищеності інформації в ІКС.***

Мета введення класифікації ІКС і стандартних функціональних

профілів захищеності й полягає у тому, щоб полегшити вирішення задачі обґрунтування вимог до ***комплексу засобів захисту (далі – КЗЗ)*** обчислювальної системи ІКС з її характеристиками.

Розуміння приналежності ІКС до певного класу і вибору стандартного функціонального профілю захищеності надають положення ***НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".***

Розглянемо вимоги цього нормативного документа. [34]

ІКС являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. *Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням ІКС.*

В цьому нормативному документі за сукупністю характеристик ІКС (конфігурація апаратних засобів ОС і їхнє фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено ***три ієрархічні класи ІКС***, ***вимоги до функціонального складу КЗЗ яких істотно різняться***.

Клас «1» – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка обробляється;

технічні засоби (носії інформації і засоби уводу/виводу) з точки зору захищеності належать до однієї категорії і всі можуть використовуватись для збереження і вводу / виводу всієї інформації.

Приклад – автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу – наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад – локальна обчислювальна мережа (далі – ЛОМ).

Клас «3» – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу – необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад – глобальна мережа.

В межах кожного класу ІКС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: ***конфіденційністю, цілісністю і доступністю***.

В зв'язку з цим, у кожному класі ІКС виділяються такі підкласи:

автоматизована система, в якій підвищені вимоги до *забезпечення конфіденційності оброблюваної інформації (підкласи «х. К»*);

автоматизована система, в якій підвищені вимоги до *забезпечення цілісності оброблюваної інформації (підкласи «х.Ц»);*

автоматизована система, в якій підвищені вимоги до *забезпечення доступності оброблюваної інформації (підкласи «х.Д»);*

автоматизована система, в якій підвищені вимоги до *забезпечення конфіденційності й цілісності оброблюваної інформації (підкласи» х.КЦ»);*

автоматизована система, в якій підвищені вимоги до *забезпечення конфіденційності й доступності оброблюваної інформації (підкласи «х.КД»);*

автоматизована система, в якій підвищені вимоги до *забезпечення цілісності й доступності оброблюваної інформації (підкласи «х.ЦД»).*

автоматизована система, в якій підвищені вимоги до *забезпечення конфіденційності, цілісності й доступності оброблюваної інформації (підкласи «х.КЦД»).*

Для кожного з підкласів кожного класу вводиться певна кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу ІКС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг.

Отже, розглянута вище класифікація необхідна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ ОС, проєктованої

або наявної ІКС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ ІКС. Однак слід визнати, що для створення КЗЗ, який найповніше буде відповідати характеристикам і вимогам до конкретної ІКС, необхідне проведення в повному обсязі аналізу загроз і оцінки ризиків безпеці інформації для цієї ІКС.

Ці питання доцільно докладніше розглянути під час практичного групового заняття.

2.2 Методичні рекомендації щодо вивчення положень основних нормативних документів щодо захищеності від несанкціонованого доступу інформації, яка не є державною таємницею, в ІКС

Із розглянутого вище матеріалу відомо, що першочерговим завданням забезпечення безпеки інформації, що обробляється в ІКС, є збереження її цілісності, що забезпечується шляхом захисту від несанкціонованого доступу до неї (*далі – НСД*). Саме через несанкціонований доступ в більшості випадків реалізуються загрози безпеці інформації.

Несанкціонований доступ (НСД) – доступ до інформації, що здійснюється з порушенням встановлених в АС правил розмежування доступу .

Іншими словами, ***НСД – це сукупність прийомів і порядок дій з метою одержання (добування) відомостей, що охороняються, незаконним протиправним шляхом та забезпечення можливості впливати на цю інформацію*** (наприклад, підмінити, знищити і т.п.).

Можливі канали НСД до інформації в ІКС.

Кожна електронна складова ІКС, що містить у собі сукупність елементів, вузлів і провідників, має джерела інформаційного сигналу і, природньо, канали доступу та витоку інформації.

Для більшості АС характерні такі штатні (законні) канали доступу до інформації:

пристрої введення (виводу) інформації;
засоби відображення інформації;
засоби документування інформації;
засоби завантаження програмного забезпечення;
машинні носії інформації;
паперові носії інформації;
зовнішні канали зв'язку.

Крім того, витік інформації через технічні засоби ІКС може також

відбуватися за рахунок:

мікрофонного ефекту елементів електронних схем;

електромагнітного випромінювання низької і високої частоти;

виникнення паразитної генерації підсилювачів різного призначення;

наведень по ланцюгах живлення електронних систем;

наведень по ланцюгах заземлення електронних систем;

взаємного впливу проводів і ліній зв'язку;

високочастотного нав'язування потужних радіоелектронних засобів і систем;

підключення до волоконно-оптичних систем зв'язку.

Зважаючи на те, що за відсутності захисту порушник може скористатися як штатними, так і позаштатними каналами доступу, можна назвати можливими каналами несанкціонованого доступу такі канали:

усі перераховані вище штатні засоби при їх використанні *законними користувачами* не за призначенням і за межами своїх повноважень;

усі перераховані вище штатні засоби при їх використанні *сторонніми особами*;

технологічні пульти й засоби керування;

внутрішній монтаж апаратури;

лінії зв'язку між апаратними засобами даної обчислювальної системи;

побічне електромагнітне випромінювання інформації з апаратури технічних засобів;

побічні наведення інформації з мережі електроживлення і шин заземлення апаратури;

побічні наведення інформації на допоміжних і сторонніх комунікаціях, сервісному устаткуванні;

відходи у вигляді паперових і машинних носіїв інформації, кинутих у сміттєвий кошик;

запам'ятовуючі пристрої, що ремонтуються, які містять залишкову інформацію.

До осіб, які можуть використати перераховані вище можливі канали НСД, варто також додати осіб з-поміж технічного обслуговуючого персоналу та інших категорій посадових осіб установи, які за певних умов можуть бути джерелом інформації або потенційним порушником.

Канали витоку інформації і способи несанкціонованого доступу до джерел конфіденційної інформації об'єктивно взаємозалежні. Кожному каналові відповідає визначений спосіб НСД.

Розуміючи суть створення можливих каналів НСД до інформації в ІКС можна розпочати вивчення положень основних нормативних документів, у яких визначені заходи захисту від несанкціонованого доступу інформації, яка не є державною таємницею.

Вивчення положень вищевказаних нормативних документів доцільно здійснити в процесі проведення групового (практичного) заняття за раніше розглянутою методикою в главі 1.3 розділу 1 посібника.

Пропонуємо наступний обсяг завдань щодо вивчення призначення та головних положень нормативних документів під час групового (практичного) заняття, а також переліки питань для проведення контролю (самоконтролю) якості вивчення матеріалу.

2.2.1 НД ТЗІ 2.5-008-2002 “Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2”

Цей нормативний документ визначає вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 і установлює згідно з визначеними НД ТЗІ 2.5-004 специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їх реалізації у комплексах засобів захисту інформації. [35]

Мета цього документа – надання нормативно-методологічної бази під час розроблення комплексів засобів захисту від НСД до конфіденційної інформації, яка обробляється в АС класу 2, створення комплексної системи захисту інформації в установі (організації), проведення аналізу та оцінки захищеності інформації від несанкціонованого доступу в системах такого класу, а також рекомендацій для визначення необхідного функціонального профілю захищеності інформації в конкретній АС.

Цей НД ТЗІ призначений для суб’єктів відносин (власників або розпорядників АС, користувачів), діяльність яких пов’язана з обробкою в автоматизованих системах конфіденційної інформації, розробників комплексних систем захисту інформації в автоматизованих системах, для постачальників компонентів АС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності АС на відповідність вимогам ТЗІ.

Вимоги цього НД ТЗІ є обов’язковими для державних органів, Збройних Сил, інших військових формувань, МВС, Ради Міністрів Автономної республіки Крим та органів місцевого самоврядування, а також підприємств, установ та організацій усіх форм власності, в АС яких обробляється конфіденційна інформація, що є власністю держави. Для конфіденційної інформації, що не є власністю держави, вимоги даного

нормативного документа суб'єкти господарської діяльності можуть використовувати на власний розсуд.

Обсяг завдань щодо роботи з положеннями НД ТЗІ 2.5-008-2002 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2":

– опрацювати НД ТЗІ у повному обсязі;

– детально опрацювати зміст п. п. 5.3, 6.1, 6.2, 6.3 (6.3.6 – особливо), 6.5, розділ 7;

Контрольні питання:

1. *Яке призначення даного НД ТЗІ?*
2. *Яким вимогам (навести перелік організаційних та інженерно-технічних заходів) повинна відповідати захищена технологія обробки інформації в ІКС (ст. 5.3)?*
3. *Які підсистеми включає функціонально-логічна структура обчислювальної системи ІКС класу 2, надати характеристику кожної із підсистем (п.п. 6.1.1 – 6.1.4)?*
4. *Які організаційні заходи передбачає облаштування фізичного середовища функціонування ІКС (п.6.2)?*
5. *Які заходи передбачає організація управління доступом до конфіденційної інформації та компонентів ІКС (п.6.3.6)?*
6. *Які заходи повинні бути реалізовані у разі виводу інформації на матеріальні носії (на аркуш паперу, на цифровий носій) (п.6.5.10, 6.5.11)?*
7. *Якщо обробка інформації в ІКС вимагає підвищених вимог до забезпечення конфіденційності оброблюваної інформації, якому стандартному профілю захищеності оброблюваної інформації повинна відповідати АС класу 2, який перелік мінімально необхідних рівнів послуг безпеки повинен забезпечуватися КЗЗ при цьому (п.6.5.15 абзац 2)?*
8. *Якщо обробка інформації в ІКС вимагає підвищених вимог до забезпечення конфіденційності та цілісності оброблюваної інформації, якому стандартному профілю захищеності оброблюваної інформації повинна відповідати АС класу 2, який перелік мінімально необхідних рівнів послуг безпеки повинен забезпечуватись КЗЗ при цьому (п.6.5.15 абзац 3)?*
9. *На які об'єкти ІКС поширюються положення Політики безпеки інформації в АС (розділ 7, вступна частина розділу)?*

Розуміння положень даного НД ТЗІ вимагає поглибленого вивчення наступного НД ТЗІ 2.5-005-99 "Порядок класифікації ІС і визначення для них стандартних функціональних профілей захищеності оброблюваної

інформації від несанкціонованого доступу”.

2.2.2 Порядок класифікації ІКС і визначення для них стандартних функціональних профілей захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5-005-99)

Вивчення положень ***НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”*** *(затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22)* в обсязі з’ясування віднесення ІКС до певних класів було розпочато раніше (розділ 2 пункт 2.1 підпункт 2.1.5).

Завданнями даного групового (практичного) заняття є *вивчення порядку визначення функціональних профілей захищеності оброблюваної інформації від несанкціонованого доступу для ІКС*. Саме положення цього НД ТЗІ і нададуть розуміння послідовності розв’язання цього завдання.

Обсяг завдань щодо роботи з положеннями ***НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”:***

– опрацювати НД ТЗІ у повному обсязі;

Контрольні питання та завдання:

1. *Що являє собою стандартний функціональний профіль захищеності (розділ 6 абзац 1)?*
2. *Поясніть семантику стандартного функціонального профілю захищеності (п. 6.2).*
3. *Надайте тлумачення стандартному функціональному профілю захищеності 2.КЦ.2.*
4. *Поясніть, що позначено у фігурних дужках праворуч від наведених стандартних функціональних профілей захищеності у розділі 7.*
5. *На Вашу думку, чи всі із наведених в розділі 7 стандартних функціональних профілей захищеності використовуються на практиці?*
6. *Ваші припущення: які із наведених в розділі 7 стандартних функціональних профілей захищеності частіше всього використовуються на практиці в ІКС державних установ (Додаток А)?*

Під час вивчення *розділу 7* НД ТЗІ 2.5-005-99 “Порядок класифікації ІС і визначення для них стандартних функціональних профілей

захищеності оброблюваної інформації від несанкціонованого доступу" виникають питання щодо тлумачення скороченої абревіатури *(була наведена у фігурних дужках кожного із вказаних стандартних функціональних профілей захищеності) рівнів гарантій захищеності, які повинен забезпечувати КЗЗ ІКС*. [34]

З'ясуванню цих питань сприяють знання положень наступного НД ТЗІ 2.5-004-99.

2.2.3 Встановлені критерії оцінки захищеності інформації в ІКС від несанкціонованого доступу (НД ТЗІ 2.5-004-99)

НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" *(затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22 зі змінами згідно з наказом Адміністрації Держспецзв'язку від 28 грудня 2012 року № 806) установлює критерії оцінки захищеності інформації, оброблюваної в ІКС, від несанкціонованого доступу.* [36]

Критерії є методологічною базою для:

– визначення вимог із захисту інформації в ІКС від несанкціонованого доступу;

– створення захищених ІКС і засобів захисту від несанкціонованого доступу;

– оцінки захищеності інформації в ІКС і їхньої придатності для обробки критичної інформації (інформації, що вимагає захисту).

Обсяг завдань щодо роботи з положеннями ***НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу":***

– вивчити призначення НД ТЗІ (ст. 1);

– ознайомитись із загальною термінологією та побудовою змісту НД ТЗІ;

– опрацювати усі статті НД ТЗІ.

Контрольні питання та завдання:

1. *Доповісти про призначення НД ТЗІ (ст. 1).*
2. *Доповісти про загальну побудову змісту НД ТЗІ (складається із 30 статей на 13 сторінках).*
3. *До яких головних категорій в даному НД ТЗІ сформульовані вимоги (п. 5 перший абзац)?*

4. *На які чотири групи розбиті функціональні критерії (критерії безпеки) (п.5 другий – п'ятий абзац)?*
5. *Скільки рівнів передбачає ієрархія критеріїв гарантій Г- .... (п. 5 шостий абзац)?*
6. *Надайте тлумачення скороченій абревіатурі НЦ-1 (п. 9.5 перша колонка, крім того: НР-1 п. 9.1 перша колонка; НО-1 п. 9.4 перша колонка).*

Отже, кожний із вивчених нормативних документів займає своє місце у загальній системі нормативно-правового забезпечення безпеки інформації під час її обробки в ІКС та має своє призначення. Однак, їх потрібно розглядати як сукупність логічно пов'язаних нормативних документів із захисту в ІКС службової та іншої конфіденційної інформації від несанкціонованого доступу.

2.3 Положення нормативно-правового забезпечення, щодо створення в ІКС комплексних систем захисту інформації, яка є державною таємницею

2.3.1 Нормативно-правове обґрунтування обов'язковості створення комплексної системи захисту інформації (далі – КСЗІ) в ІКС

Нормативно-правове обґрунтування обов'язковості створення комплексної системи захисту інформації в ІКС починається із положень таких головних Законів України у сфері інформаційних відносин, вимоги яких були розглянуті вище:

Закон України "Про інформацію" від 02 жовтня 1992 року № 2657-XII (зі змінами);

Закон України "Про державну таємницю" від 21 січня 1994 року № 3856-XII (зі змінами);

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05 липня 1994 року № 80/94-ВР (зі змінами).

У статті 21 Закону України "Про інформацію" від 02 жовтня 1992 року № 2657-XII (зі змінами) визначені вимоги щодо обов'язкового врегулювання в державі на законодавчому рівні порядку доступу осіб інформації, яка становить державну таємницю.

Такий особливий порядок доступу осіб до державної таємниці, а також заходи щодо охорони державних секретів та відповідальність осіб за порушення законодавства про державну таємницю встановлюються

вимогами Закону України “Про державну таємницю” від 21 січня 1994 року № 3856-XII (зі змінами). Доцільно звернути увагу на заключні положення цього закону щодо відповідальності посадових осіб та громадяни за порушення законодавства про державну таємницю (передостанній та останній абзаци ст. 39 Закону): [18]

“у невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності таємної інформації або просочення її технічними каналами, – несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом”.

Ці вимоги Закону України “Про державну таємницю” від 21 січня 1994 року № 3856-XII (зі змінами) конкретизуються та підсилюються вимогами НПА загальнодержавного використання “Порядком організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, підприємствах, в установах і організаціях” (введеного в дію постановою КМУ від 18.12.2013 № 939**).** Головні положення цього НПА добре відомі здобувачам вищої освіти із курсу освітнього компонента “*Основи організації та забезпечення режиму секретності в установах і організаціях України”***,** а самі вимоги є повсякденними нормами здійснення навчального процесу в інституті із спеціальних дисциплін.

Для визначення приналежності певної інформації до державної таємниці і встановлення відповідного ступеня обмеження доступу до неї здобувачі вищої освіти вже навчені використовувати положення “Зводу відомостей, що становлять державну таємницю”(ЗВДТ-2020), затвердженого наказом Центрального управління Служби безпеки України від 23.12.2020 № 383, зареєстрованого в Міністерстві юстиції України 14.01.2021 за № 52/35674.

Ґрунтуючись на положеннях вище наведених законів та НПА, абсолютну ясність щодо *обов’язковості створення комплексної системи захисту інформації в ІС у разі обробки секретної інформації* вносять вимоги Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05 липня 1994 року № 80/94-ВР (зі змінами). Ці вимоги містяться у положеннях ст. 8 даного Закону: [13]

“*Стаття 8. Умови обробки інформації в системі.*

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням ***комплексної системи захисту інформації з підтвердженою відповідністю.*** *Підтвердження*

відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством".

У положеннях ст. 16 НПА ***"Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" (постанова КМУ від 29 березня 2006 року № 373, зі змінами),*** встановлені завдання та вимоги до комплексної системи захисту інформації (далі – КСЗІ), а саме: [32]

"Для забезпечення захисту інформації в системі створюється ***комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:***

витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації ***від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту ухвалене розпорядником інформації.***

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту ухвалене розпорядником інформації.

. . . . . .

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи."

Отже, у разі організації обробки засобами інформаційно-комунікаційної системи інформації, яка становить державну таємницю, відповідно до вимог чинного законодавства України, рішенням керівника організації, яка є власником (розпорядником) системи, в ній обов'язково

створюється комплексна система захисту інформації. Ця КСЗІ повинна забезпечити захист інформації від:

витоку технічними каналами (ПЕМВН, акустично-електричні та інші);

несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів.

За окремим рішенням розпорядника інформації КСЗІ повинна також забезпечити захист інформації від спеціального впливу на засоби обробки інформації.

Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Сформульовані вимоги до КСЗІ вимагають більш докладного розгляду технічних каналів можливого витоку інформації в ІКС, природи та причин їх об’єктивного існування.

2.3.2 Технічні канали витоку інформації. Обґрунтування необхідності впровадження заходів технічного захисту інформації

Розгляд походження технічних каналів витоку інформації доцільно розпочати із з’ясування суті наступних базових термінів та понять:

Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

Витік інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Канали витоку інформації – методи та шляхи витоку інформації з інформаційної системи; паразитний (небажаний) ланцюжок носіїв інформації, один або кілька з яких є або можуть бути використані правопорушником або його спеціальною апаратурою.

Технічний канал витоку інформації (далі – ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки.

Канал витоку можна представити таким, що складається з джерела створення сигналу, фізичного середовища його розповсюдження до приймальної сторони (зловмисника, конкурента тощо) і приймальної апаратури, що за функціональним призначенням, можливостями і тактико-технічними характеристиками відрізняється від апаратури, яка застосовується в каналі передачі інформації. В даному випадку рух інформації здійснюється від джерела інформації до зловмисника, тобто є одностороннім. З урахуванням такого зауваження визначимо *канал витоку*

інформації як фізичний шлях від джерела інформації до зловмисника, через який несанкціоновано можуть бути одержані конфіденційні відомості.

Очевидно, що для створення каналу витоку інформації необхідні відповідні просторові, енергетичні і часові умови, а також відповідні засоби прийому і фіксації інформації на боці зловмисника (рис. 2.1):

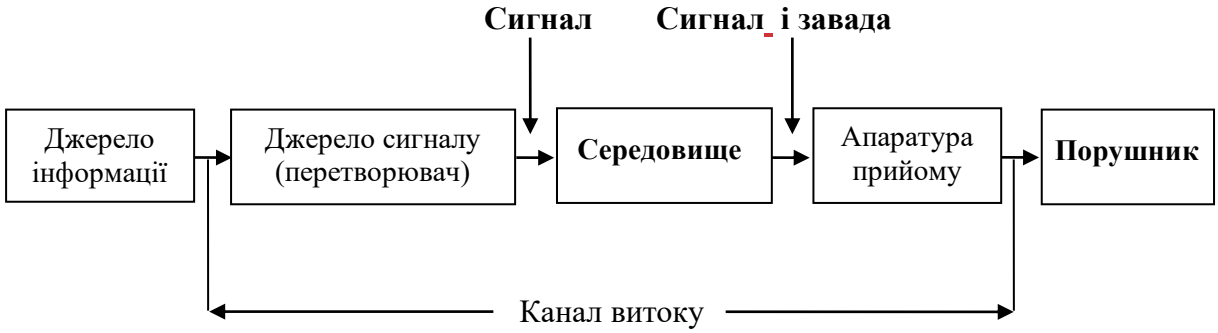


Рис. 2.1. Структурна схема каналу витоку інформації

Слід зазначити, що при розгляді *технічних каналів витоку* інформації сигнал, що створюється перетворювачем і несе відомості (інформацію) з обмеженим доступом, заведено називати **небезпечним сигналом**, а перетворювач, що створює цей сигнал – **джерелом небезпечного сигналу**. Таким джерелом можуть бути технічні засоби, їхні елементи, вузли, блоки, що знаходяться в експлуатації і при цьому створюють певні фізичні поля, що несуть інформацію з обмеженим доступом, отримання якої порушником можливе за певних обставин.

Залежно від способу доступу до інформації, канали витоку поділяються на два види – *прямі й непрямі*.

Непрямі канали витоку інформації – це такі канали, використання яких для несанкціонованого доступу до інформації не потребує проникнення у приміщення, де здійснюється її обробка.

Прямі канали витоку інформації передбачають безпосередній доступ до інформації, яка обробляється. При цьому прямі канали можуть використовуватись без зміни структури елементів системи обробки інформації або зі зміною цієї структури.

Серед можливих каналів витоку інформації найбільш небезпечними з точки зору її отримання, аналізу і виділення корисної інформації є **технічні канали витоку**, які можуть бути *самочинними* (ненавмисними), в яких носії інформації та (чи) середовище її поширення формуються самочинно (ненавмисно), та *штучними* (навмисними).

Фізичні процеси, що відбуваються у технічних засобах у процесі їхнього функціонування, створюють у навколишньому середовищі побічні випромінювання, які тією чи іншою мірою пов`язані з інформацією, що обробляється. Фізичні явища, що лежать в основі появи цих випромінювань, мають різний характер, але водночас вони можуть розглядатись, як ненавмисна передача інформації з обмеженим доступом по деякій "побічній системі зв`язку", створеній джерелом небезпечного випромінювання, середовищем і, можливо, приймальною стороною (зловмисником). При цьому, на відміну від традиційних систем зв`язку, в яких передавальна і приймальна сторони прагнуть однієї мети – передати і прийняти інформацію з найбільшою достовірністю, у випадку "побічної системи зв`язку" передавальна сторона зацікавлена у можливо більшому погіршенні (послабленні, ліквідації, спотворенні, викривленні) інформації, що передається, оскільки це сприяє її захисту, а приймальна сторона намагається максимально покращити умови прийому інформації, яка її вкрай цікавить.

Таку "побічну систему зв`язку" заведено називати *технічним каналом витоку інформації*. Правомірно передбачити, що створенню ТКВІ сприяють певні обставини й причини технічного характеру, наприклад недосконаліть елементної бази і схемних рішень, прийнятих для даної категорії технічних засобів, експлуатаційний знос елементів виробу, а також зловмисні дії тощо (рис. 2.2):

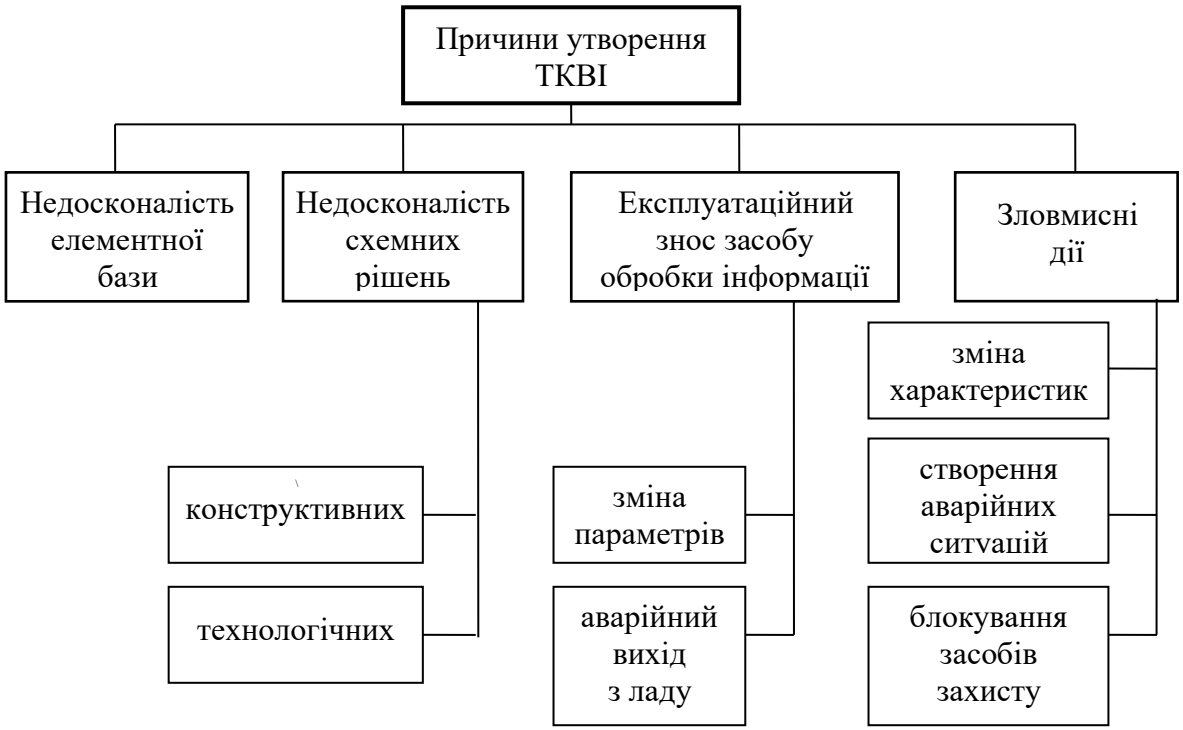


Рис. 2.2. Причини утворення технічних каналів витоку інформації

За *фізичною природою* канали витоку інформації можливо розділити на такі групи (рис. 2.3):

матеріально-речовинні (папір, фото- і магнітні носії тощо);
візуально-оптичні (спостереження, фотографування тощо);
акустичні (зокрема й акустоперетворюючі);
електромагнітні (в тому числі магнітні й електричні).

Ця сукупність технічних каналів витоку є базовою.



Рис. 2.3. Класифікація ТКВІ за фізичною природою

Залежно від форми представлення інформації розрізняють і технічні канали її витоку, які характерні тільки для певної форми і мають свої особливості.

Так, для *документальної* інформації основними технічними каналами її витоку є матеріально-речовинні й візуально-оптичні канали.

Для *телекомунікаційної* інформації технічними каналами витоку можуть бути електромагнітні, електричні й параметричні канали.

Для *мовної* інформації технічними каналами витоку є повітряні (прямі акустичні), вібраційні (віброакустичні), електроакустичні, оптико-електронні і параметричні канали.

Для ІКС характерними технічними каналами витоку інформації є:

А. ТКВІ мовної інформації:
акустичні;
акустовібраційні (віброакустичні);
акустооптоелектричні (лазерні акустичні);
відео акустичні;
канали ВЧ нав’язування;
канали витоку мовної інформації на основі закладних пристроїв.

Б. ТКВІ, що обробляється в ОТЗС:
канали побічних електромагнітних випромінювань;
канали побічних електромагнітних наведень;
канали “паразитної” модуляції сигналів ВЧ генераторів;
канали “паразитної” ВЧ генерації підсилювачів;
канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних;
канали перехоплення (зняття) інформації з каналів зв’язку;
канали ВЧ нав’язування;
канали витоку інформації на основі закладних пристроїв.

Фізичне обґрунтування об’єктивного існування вищенаведених ТКВІ вам відоме із курсу освітнього компонента “Технічний захист інформації”.

Отже, функціонування ІКС об’єктивно пов’язане з існуванням цілої низки технічних каналів витоку інформації, яка в ній обробляється. З огляду на те, що зміст інформації складає державну таємницю, можливий витік інформації розглядається як порушення вимог законодавства з охорони державної таємниці із встановленою законодавством відповідальністю певних посадових осіб. З метою недопущення витоку інформації впроваджується КСЗІ, як взаємопов'язана

сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації в ній.

Нормативно-правове забезпечення та загальний порядок проведення робіт із технічного захисту інформації на ОІД (в тому числі й побудови КСЗІ в ІС), розглянемо у наступному підпункті 2.3.3.

2.3.3 Загальний порядок проведення робіт із технічного захисту інформації в ІС (ДСТУ 3396.0-96, ДСТУ 3396.1-96)

Загальний порядок проведення робіт із побудови КСЗІ в ІС регламентується положеннями основних Державних Стандартів України у сфері технічного захисту інформації, а саме:

ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення";

ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт".

ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення" установлює об'єкт, мету, основні організаційно технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян-суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

ДСТУ 3396.0-96 встановлює єдиний порядок проведення робіт із технічного захисту інформації на ОІД, незалежно від їхнього долучення до створення КТЗІ чи КСЗІ.

Даним стандартом визначається: [39]

П. 3.6. Метою ТЗІ є запобігання витоку або порушенню цілісності ІзОД.

П. 3.7 Мета ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ. Технічний захист інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціювання та керування системою захисту інформації.

У подальших пунктах ДСТУ деталізуються вимоги до системи захисту інформації на ОІД.

В положеннях ***ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт"*** підтверджується встановлений ДСТУ 3396.0-96 порядок проведення робіт із технічного захисту інформації на ОІД, а також визначається із певним ступенем деталізації послідовність реалізації етапів виконання робіт.

Зокрема, положеннями ДСТУ 3396.1-96 визначено: [40]

П. 3.3. Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам функціювання системи захисту інформації і полягає в:

- проведенні обстеження підприємства, установи, організації (далі – підприємство);

- розробленні й реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ (додаток А);

- прийманні робіт з ТЗІ;

- атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

П. 3.4 Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства.

Роботи повинні виконуватися силами підприємства під керівництвом спеціалістів з ТЗІ.

Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ інших організацій, які мають ліцензію органу, уповноваженого Кабінетом Міністрів України.

У подальших розділах та пунктах даного стандарту визначений порядок реалізації заходів із створення системи захисту інформації на ОІД, а саме:

Розділ 4 – Організація проведення обстеження підприємства:

створення комісії;

які питання підлягають обстеженню;

документування результатів обстеження (акт, додатки до акту).

Розділ 5 – Організація розроблення системи захисту інформації:

узагальнення інформації моделі загроз та результатів обстеження;

відпрацювання технічного завдання на розроблення системи захисту інформації;

відпрацювання плану захисту інформації (перелік документів).

Розділ 6 – Реалізація організаційних заходів захисту:
визначення переліку організаційних заходів захисту;
організація керування системою захисту інформації;
Розділ 7 – Реалізація первинних технічних заходів захисту:
завдання первинних технічних заходів;
послідовність реалізації первинних технічних заходів;
Розділ 8 – Реалізація основних технічних заходів захисту:
перелік основних технічних заходів захисту;
вибір засобів забезпечення ТЗІ, загальні вимоги до них, порядок застосування;
Розділ 9 – Приймання, визначення повноти та якості робіт:
приймання виконаних робіт (складання акту);
порядок проведення атестації системи захисту інформації.

Розглянуті вище положення основних стандартів ДСТУ 3396.0-96 та ДСТУ 3396.1-96, доповнюючи положення один одного, визначають єдиний загальний порядок проведення робіт з технічного захисту інформації на ОІД установ. А чи достатньо цих відомостей для того щоб, керуючись їхніми положеннями, починати роботу щодо створення та упровадження КСЗІ в ІКС? Вочевидь, ні. Хоча і зрозумілий загальний напрямок та етапи робіт, але цього недостатньо. Потрібна інформація більш детальна, яка б надавала уявлення послідовного покрокового виконання заходів кожного етапу, а також враховувала призначення та характеристики конкретного ОІД, складу основних технічних засобів обробки інформації (ОТЗ), переліку та особливостей додаткових технічних засобів та систем (ДТЗС), технологій обробки інформації на ОІД, переліку наявних ризиків (загроз) для безпеки інформації тощо.

В наступних главах даного розділу послідовно будемо шукати відповіді на всі ці питання у вимогах чинних нормативних документів з ТЗІ, таких як:

НД ТЗІ 3.7-003-2023 "Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі";

НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі";

НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі" та інші.

Отже, ми розглянули положення основних нормативно-правових актів та нормативних документів України щодо створення в ІКС комплексних систем захисту інформації, яка є державною таємницею,

обґрунтували обов'язковість їх створення, з'ясували загальну послідовність виконання робіт.

Із розглянутого вище матеріалу можна зробити певні припущення щодо багатоплановості, чималого загального обсягу та складності робіт, пов'язаних із побудовою КСЗІ в ІКС, а також висновки щодо необхідності системного та поглибленого вивчення вимог НПА та нормативних документів, чинних у сфері ТЗІ.

2.4 Положення нормативно-правового забезпечення щодо організації технічного захисту інформації в Україні

У попередніх главах розділу 2 були розглянуті положення законодавчих, нормативно-правових та нормативних документів, вимогами яких встановлюється обов'язковість впровадження в ІКС, в яких обробляються державні інформаційні ресурси *систем захисту інформації*. А коли йдеться про обробку інформації, що складає державну таємницю, положення НПА вимагають створення *комплексних систем захисту інформації*, які призначені для захисту інформації від витоку усіма можливими каналами (в тому числі й каналами ПЕМВН).

Виникає закономірне питання: а створення систем захисту інформації стосується тільки процесів її обробки в ІКС? Відповідь: звичайно, ні! Питання стоїть набагато ширше і його необхідно розглядати у певній історичній хронології розвитку інформаційних технологій в державі.

Впровадження заходів технічного захисту, як один із напрямків забезпечення безпеки інформації, розглядалися завжди. У 1991 році після набуття незалежності Україна стала на складний шлях побудови нової демократичної держави. У середині 90-х років із прийняттям концепції стрімкої інформатизації усіх сфер діяльності суспільства із широким впровадженням сучасних інформаційних технологій автоматизованої обробки та передачі інформації, лібералізацією суспільних та міждержавних відносин на тлі кризового стану економіки, зросли загрози для інформації, гостро постала проблема забезпечення її безпеки. Закономірно на державному рівні стало на часі питання щодо визначення загальної концепції технічного захисту інформації в Україні, та створення відповідного нормативно-правового забезпечення в цьому секторі ІБ держави.

Так, постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126 була ухвалена "Концепція технічного захисту інформації в Україні".

2.4.1 Положення “Концепції технічного захисту інформації в Україні” (прийнято постановою Кабінету Міністрів України від 8 жовтня 1997 року № 1126)

Концепція визначила основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації (далі – ТЗІ) став складовою частиною забезпечення національної безпеки України. [43]

Концепція задекларувала єдність принципів формування і проведення державної політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) і стала правовою підставою для створення програм розвитку сфери ТЗІ в державі.

В концепції було сформульовано визначення ТЗІ:

ТЗІ – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Положення Концепції були спрямовані на узгодження інформаційних відносин у сфері ТЗІ з міжнародними стандартами та сприяння утвердженню України у світі як демократичної правової держави. У зв'язку з цим в Концепції відповідним чином були сформульовані принципи формування і проведення державної політики у сфері ТЗІ, а також основні функції організаційних структур системи ТЗІ (*у розділі 3).*

Даний НПА визначив пріоритетні напрями державної політики у сфері ТЗІ (*у розділі 4*):

1. Удосконалення всієї системи нормативно-правового забезпечення в цьому секторі (стосовно всіх видів інформації: відкритої, конфіденційної, службової, ДТ).

2. Удосконалення правових механізмів організаційного забезпечення ТЗІ:

забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

підготовка кадрів для роботи у сфері ТЗІ;

залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

3. Розвиток міжнародного співробітництва в сфері ТЗІ;

4. Вдосконалення науково-технічної та виробничої діяльності в сфері ТЗІ:

моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

обґрунтування критеріїв та показників рівнів ТЗІ;

створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Визначені ***першочергові заходи щодо реалізації державної політики у сфері ТЗІ***:

створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;

визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;

налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення,

оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;

завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;

визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Ухвалення *"Концепції технічного захисту інформації в Україні"* потужно зрушила з місця діяльність суб'єктів інформаційних відносин, науково-технічного та виробничого потенціалу міністерств, відомств, інших центральних органів виконавчої влади щодо реалізації державної політики у секторі ТЗІ в усіх визначених напрямках. Потужний імпульс отримала діяльність з нарощування та удосконалення всієї системи нормативно-правового забезпечення ТЗІ.

2.4.2 "Положення про технічний захист інформації в Україні" (указ Президента України від 27 вересня 1999 року № 1229/99)

Наступним важливим нормативно-правовим актом конституційного рівня у секторі ТЗІ стало ***"Положення про технічний захист інформації в Україні", яке було ухвалено указом Президента України від 27 вересня 1999 року № 1229/99*** *(далі – Положення).*

Положення мало на меті визначити правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства. [44]

Цим НПА встановлена обов'язковість впровадження технічного захисту інформації органами державної влади, органами місцевого самоврядування, органами управління Збройних Сил України та іншими військовими формуваннями, утвореними згідно із законодавством України, підприємствами, установами, організаціями, із покладанням відповідальності за здійснення ТЗІ на їхніх керівників.

Положенням були встановлені вимоги щодо фінансування із державного бюджету комплексу заходів із розроблення, видання нормативно-правових актів з питань технічного захисту інформації, а також робіт, пов'язаних з розробленням і виконанням загальнодержавних програм розвитку ***системи технічного захисту інформації.***

У НПА були також визначені суб'єкти системи ТЗІ – важливої складової системи ТЗІ держави (п. 8), їх завдання та функції (п. п. 11, 12):

Суб'єктами системи технічного захисту інформації є:

***Держспецзв'язку України**;*

органи, щодо яких здійснюється ТЗІ;

науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

здійснення контролю за станом технічного захисту інформації.

Органи, щодо яких здійснюється ТЗІ:

створюють (визначають) підрозділи, на які покладається забезпечення технічного захисту інформації та контроль за його станом, узгоджують основні завдання та функції цих підрозділів;

видають за погодженням з Адміністрацією Держспецзв'язку України та впроваджують нормативно-правові акти з питань технічного захисту інформації;

погоджують з Адміністрацією Держспецзв'язку України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи технічного захисту інформації, які здійснюються за рахунок коштів державного бюджету;

створюють або визначають за погодженням з Адміністрацією Держспецзв'язку України підприємства, установи та організації, що забезпечують технічний захист інформації;

забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з технічного захисту інформації;

надають Адміністрації Держспецзв'язку України за його запитами відомості про стан технічного захисту інформації.

В НПА визначені основні завдання й іншим суб'єктам системи технічного захисту інформації (п. 13).

В подальших пунктах положення були визначені принципи та механізми функціонування системи ТЗІ держави за такими

напрямками:

обов’язковість засвідчення у встановленому порядку відповідності технічних засобів загального використання матеріально-технічної бази системи ТЗІ (п. 15);

обов’язковість використання під час впровадження заходів з технічного захисту інформації тільки технічних засобів, які дозволені Адміністрацією Держспецзв'язку України для застосування та включених до відповідних переліків (п. 17);

обов’язковість впровадження ТЗІ під час здійснення робіт з техніко-економічного обґрунтування, проєктування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій (п. 16);

організація та проведення контролю у сфері технічного захисту (п. п. 18, 19);

порядок розроблення, впровадження, атестація та експлуатація комплексів технічного захисту інформації для власних потреб (п. 20);

порядок фінансування робіт з технічного захисту інформації в органах, щодо яких здійснюється ТЗІ (п. 21);

встановлення відповідальності посадових осіб та громадян у разі порушення вимог щодо забезпечення технічного захисту інформації (п. 22).

Отже, “Положення про технічний захист інформації в Україні”, яке було ухвалено указом Президента України від 27 вересня 1999 року № 1229/99, визначило головні правові та організаційні засади технічного захисту важливої для держави, суспільства й особи інформації; обов’язковість впровадження ТЗІ відносно такої інформації усіма суб’єктами інформаційних відносин; завдання, права та обов’язки суб’єктів системи ТЗІ щодо впровадження державної політики в цьому секторі ІБ; принципи та механізми функціонування системи ТЗІ держави.

Положення даного НПА стали, у певному сенсі, каталізатором подальшого процесу нарощування системи нормативно-правового забезпечення ІБ певною кількістю нормативних документів ТЗІ, призначених для впровадження способів та заходів ТЗІ на ОІД, норм та методик перевірки захищеності інформації, методик проведення контролю стану ТЗІ тощо.

2.4.3 Обґрунтування необхідності створення комплексів технічного захисту інформації (далі – КТЗІ) на об’єктах інформаційної діяльності установ.

В результаті аналізу вимог вище розглянутої низки законодавчих, нормативно-правових актів та нормативних документів, випливають такі обґрунтовані твердження:

1. На об’єктах інформаційної діяльності інформація може циркулювати у вигляді сигналів, сформованих різними фізичними полями (акустичними, магнітними, електричними, електромагнітними). Термін “інформація циркулює” означає: її створення, введення, збирання, записування, передавання, приймання (отримання), копіювання, перетворення, реєстрацію, розмноження, сканування (зчитування), роздрукування, зберігання, відображення будь-яким чином, виготовлення (друкування) графічних та текстових документів, знищення тощо;
2. У разі, коли на певному об’єкті циркулює інформація з обмеженим доступом (ІзОД), яка є власністю держави, власник цього об’єкта зобов’язаний вжити заходів ТЗІ з метою запобіганню її можливого витоку технічними каналами, а також внаслідок НСД;
3. Обов’язковому захисту від витоку технічними каналами підлягає інформація, що становить державну таємницю;
4. Захист іншої інформації з обмеженим доступом від витоку технічними каналами здійснюється за рішенням розпорядника (користувача) цієї інформації у порядку та за вимогами, встановленими для захисту секретної інформації, якщо інше не встановлено законодавством України.
5. У разі порушення вимог щодо забезпечення технічного захисту інформації посадовими особами та громадянами встановлена відповідальність відповідно до чинного законодавства.

Для захисту інформації, що становить державну таємницю або іншої інформації з обмеженим доступом (за рішенням розпорядника інформації) від витоку технічними каналами створюється та атестується ***комплекс технічного захисту інформації (далі – комплекс ТЗІ, КТЗІ)***.

Комплекс ТЗІ – це сукупність заходів та засобів, призначених для реалізації технічного захисту інформації на об’єкті інформаційної діяльності (далі –.ОІД).

Комплекс ТЗІ створюється (модернізується) *за рішенням (наказом, розпорядженням) керівника установи-замовника* про:

створення комплексу ТЗІ на ОІД установи для захисту секретної мовної інформації;

створення комплексної системи захисту секретної інформації в ІКС у разі потреби її обробки технічними засобами (в цьому випадку КТЗІ розглядається як складова КСЗІ).

Комплекс ТЗІ може створюватися також на виконання *рішення розпорядника (користувача) іншої інформації з обмеженим доступом* щодо її захисту від витоку технічними каналами.

Модернізація комплексу ТЗІ здійснюється у разі змін умов функціонування ОІД (ІКС) або необхідності змін умов обробки та/або озвучування інформації.

Етапи створення та порядок експлуатації комплексів ТЗІ здобувачі вищої освіти докладно будуть вивчати у подальшому навчальному процесі на заняттях освітніх компонент "Технічний захист інформації", "Системи та комплекси технічного захисту інформації", "Убезпечення інформації від витоку технічними каналами".

2.5 Положення нормативно-правового забезпечення щодо створення та супроводження функціонування КСЗІ в ІКС

Успішне вирішення складних та багатопланових завдань, пов'язаних із побудовою, супроводженням функціонування КТЗІ на ОІД (або КСЗІ в ІКС), встановлена відповідальність посадових осіб за виконання вимог з ТЗІ, потребують залучення для виконання цих завдань фахівців із відповідним рівнем їхньої підготовки. Це може бути забезпечено за наявності в установі підрозділу технічного захисту інформації (служби захисту інформації) установи, до складу якого входять такі фахівці із визначеними обов'язками та повноваженнями.

Створення та функціонування такого спеціалізованого підрозділу (служби) в установі повинно мати чітке юридичне обґрунтування та забезпечуватись відповідними нормативно-правовими актами держави.

2.5.1 Вимоги нормативно-правових актів щодо створення підрозділів (служб) технічного захисту інформації

Нормативно-правове обґрунтування *обов'язковості створення підрозділів (служб) технічного захисту інформації* випливає із положень наступних головних законодавчих, НПА та нормативних документів України у сфері інформаційних відносин та технічного захисту інформації, вимоги яких були вивчені на попередніх заняттях:

Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05 липня 1994 року № 80/94-ВР (зі змінами);

“Концепції технічного захисту інформації в Україні”, введеної в дію постановою КМУ від 08 жовтня 1997року № 1126;

“Положення про технічний захист інформації в Україні”, введеного в дію указом Президента України від 27 вересня 1999 року № 1229/99;

“Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”, введених в дію постановою КМУ від 18 грудня 2013 року № 373, (зі змінами);

НД ТЗІ 3.7-003-2023 “Порядку проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі”.

Розглянемо ці вимоги.

Так, відповідно до вимог *статті 9 Забезпечення захисту інформації в системі Закону України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05 липня 1994 року № 80/94-ВР (зі змінами)* відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

При цьому власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, *утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним*.

У положеннях *розділу 4 Основні напрями державної політики у сфері ТЗІ “Концепції технічного захисту інформації в Україні”, введеної в дію постановою КМУ від 08 жовтня 1997року № 1126*, визначено, що одним з основних напрямів державної політики у сфері ТЗІ з питань організаційного забезпечення є *забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту.* Тобто ці органи мають бути передбачені штатними розписами установ, укомплектовані відповідними фахівцями із визначеними повноваженнями у сфері ТЗІ.

Відповідно до вимог *статті 12 “Положення про технічний захист інформації в Україні”, введеного в дію указом Президента України від 27 вересня 1999 року № 1229/99* одними із першочергових завдань у сфері ТЗІ органів, щодо яких здійснюється ТЗІ, є створення (або визначення) *підрозділів ТЗІ, на які покладається забезпечення технічного захисту*

інформації та контроль за його станом. Цим підрозділам повинні бути визначені відповідні завдання та функції.

Пунктом 18 "Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах", введених в дію постановою КМУ від 18 грудня 2013 року № 373, *(зі змінами)* визначено, що *організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проєктування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.*

У положеннях *п. 5.1. НД ТЗІ 3.7-003-2023 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі", затвердженого наказом Адміністрації Держспецзв'язку від 28 жовтня 2023 року № 924*, як і в положеннях вище розглянутих НПА держави, також визначається, *що для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації*. *СЗІ повинна бути створена після ухвалення рішення про необхідність створення КСЗІ* (у крайньому випадку, як виняток, СЗІ може створюватися на більш пізніх етапах робіт, але не пізніше етапу підготовки КСЗІ до введення в дію). [41]

Хоча така обмовка про виняткові обставини викликає закономірне питання: хто в установі разом із керівником буде головним ініціатором, координатором та головним виконавцем всієї низки заходів щодо створення та упровадження КСЗІ? А ця робота потребує титанічних зусиль та певної тривалої кропіткої роботи на кожному етапі створення КСЗІ.

Зробивши аналіз положень вище наведених законодавчих, НПА та нормативних документів, узагальнивши практичний досвід побудови та супроводження КСЗІ в ІКС державних установ, зробимо висновки, які у подальшому будемо розглядати як аксіому у сфері ТЗІ:

– у разі ухвалення рішення керівником щодо розгортання в установі ІКС, в якій передбачається обробка інформації, що складає державну таємницю, ним негайно приймаються заходи щодо створення в установі підрозділу з технічного захисту інформації / служби захисту інформації (далі – СЗІ);

– керівник затверджує *Положення про СЗІ установи*, в якому визначаються: перелік НПА, на підставі вимог яких здійснюється діяльність служби; завдання, функції (повноваження) та відповідальність посадових осіб служби на всіх етапах створення та супроводження комплексної системи захисту інформації в ІКС, яка планується до розгортання;

– з призначенням на посади у СЗІ підготовлених фахівців можна розпочинати заходи щодо створення комплексної системи захисту інформацій в ІКС.

Таким чином, підставою для створення служби захисту інформації є положення вище розглянутих законодавчих, нормативно-правових та нормативних документів держави, чинних у сфері технічного захисту інформації, що регламентують питання побудови системи технічного захисту інформації та проведення робіт стосовно створення КСЗІ. Створення служби захисту інформації в установі є не тільки юридично обґрунтованим, а й об'єктивно необхідним важливим організаційним заходом.

2.5.2 Призначення та завдання служби захисту інформації установи

Призначення служби захисту інформації установи

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи у відповідності до вимог ***НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі",*** *(затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 року № 53 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28 грудня 2012 року № 806)* (далі – *Положення*). У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Відповідно до вимог п. 6.2. НД ТЗІ 1.4-001-2000 служба захисту інформації *є штатним* (у деяких виключних випадках – позаштатним) підрозділом організації. [45]

Залежно від обсягів і особливостей завдань СЗІ, до її складу можуть входити спеціалісти (групи спеціалістів, підрозділи та ін.) різного фаху:

- спеціалісти з питань захисту інформації від витоку технічними каналами;
- спеціалісти з питань захисту каналів зв'язку і комутаційного обладнання, налагодження і керування активним мережевим обладнанням;
- спеціалісти з питань адміністрування засобів захисту, керування базами даних захисту;
- спеціалісти з питань захищених технологій обробки інформації.

Метою створення служби ЗІ *є організаційне забезпечення завдань керування комплексною системою захисту інформації (далі – КСЗІ) в ІКС*

та здійснення контролю за її функціонуванням. На службу ЗІ покладається виконання робіт із організації забезпечення захисту інформації в ІКС, проєктування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІКС.

Правову основу для створення і діяльності служби ЗІ становлять Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, “Положення про технічний захист інформації в Україні”, “Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах”, “Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”.

Служба ЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими, нормативними та іншими документами установи (організації).

СЗІ здійснює діяльність відповідно до “Плану захисту інформації в автоматизованій системі”, календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) організації.

У своїй роботі служба ЗІ взаємодіє з підрозділами організації (РСО, службою безпеки, та ін.), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

Для проведення окремих заходів з захисту інформації в АС, які пов’язані з напрямком діяльності інших підрозділів організації, керівник організації своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

У разі потреби, до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

Завдання, функції, повноваження та відповідальність служби захисту інформації

Завданнями Служби ЗІ є:

захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;

дослідження технології обробки інформації в АС з метою виявлення

можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

організація та координація робіт, пов'язаних з захистом інформації в АС, необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

розроблення проєктів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в АС;

організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу АС;

участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів АС з питань захисту інформації;

формування у персоналу й користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;

організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в АС та проведення контрольних перевірок їх виконання.

Функції служби захисту інформації

Функції під час створення комплексної системи захисту інформації:

визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в АС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в АС;

розробка та коригування моделі загроз і моделі захисту інформації в АС, політики безпеки інформації в АС;

визначення і формування вимог до КСЗІ;

організація і координація робіт з проєктування та розробки КСЗІ, безпосередня участь у проєктних роботах з створення КСЗІ;

підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

вибір організацій-виконавців робіт з створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з підрозділом ТЗІ (РСО, службою безпеки

організації) погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проєкти, програма і методика випробувань, плани робіт та інш.);

участь у розробці нормативних документів, чинних у межах організації і АС, які встановлюють дисциплінарну відповідальність за порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;

участь у розробці нормативних документів, чинних у межах організації і АС, які встановлюють правила доступу користувачів до ресурсів АС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.).

Функції під час експлуатації комплексної системи захисту інформації:

організація процесу керування КСЗІ;

розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

вжиття заходів у разі виявлення спроб несанкціонованого доступу до ресурсів АС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

організація керування доступом до ресурсів АС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);

спостереження (реєстрація і аудит подій в АС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації КСЗІ;

організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ;

участь в роботах з модернізації АС – узгодженні пропозицій з введення до складу АС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

забезпечення супроводження і актуалізації еталонних, архівних і

резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

аналітичне оцінювання поточного стану безпеки інформації в АС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);

інформування власників інформації про технічні можливості захисту інформації в АС і типові правила, встановлені для персоналу і користувачів АС;

негайне втручання в процес роботи АС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

регулярне подання звітів керівництву організації-власника (розпорядника) АС про виконання користувачами АС вимог з захисту інформації;

аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для організації;

контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, у тому числі контроль за забезпеченням режиму секретності у разі обробки в АС інформації, що становить державну таємницю;

контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

розробка і реалізація спільно з РСО (підрозділом ТЗІ, службою безпеки) організації комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів та ін., здійснення їхнього технічного та інформаційного забезпечення.

Функції з організації навчання персоналу з питань забезпечення захисту інформації:

розроблення планів навчання і підвищення кваліфікації спеціалістів СЗІ та персоналу АС;

розроблення спеціальних програм навчання, які б враховували особливості технології обробки інформації в організації (АС), необхідний рівень її захищеності та ін.;

участь в організації і проведенні навчання користувачів і персоналу АС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

взаємодія з державними органами, учбовими закладами, іншими

організаціями з питань навчання та підвищення кваліфікації;

участь в організації забезпечення навчального процесу необхідною матеріальною базою, навчальними посібниками, нормативно-правовими актами, нормативними документами, методичною літературою та інш.

Повноваження та відповідальність служби захисту інформації

Служба ЗІ має право:

здійснювати контроль за діяльністю будь-якого структурного підрозділу організації (АС) щодо виконання ним вимог нормативно-правових актів і нормативних документів з захисту інформації;

подавати керівництву організації пропозиції щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки, тощо у випадку виявлення порушень політики безпеки або у випадку виникнення реальної загрози порушення безпеки;

складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;

проводити службові розслідування у випадках виявлення порушень;

отримувати доступ до робіт та документів структурних підрозділів організації (АС), необхідних для оцінки вжитих заходів з захисту інформації та підготовки пропозицій щодо їхнього подальшого удосконалення;

готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інших організацій;

готувати пропозиції щодо забезпечення АС (КСЗІ) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;

виходити до керівництва організації з пропозиціями щодо подання заяв до відповідних державних органів на проведення державної експертизи КСЗІ або сертифікації окремих засобів захисту інформації;

узгоджувати умови включення до складу АС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС;

надавати висновки з питань, що належать до компетенції служби ЗІ, які необхідні для здійснення виробничої діяльності організації, особливо технологій, доступ до яких обмежено, інших проєктів, що потребують технічної підтримки з боку співробітників СЗІ;

виходити до керівництва організації з пропозиціями щодо узгодження планів і регламенту відвідування АС сторонніми особами;

інші права, які надані службі ЗІ у відповідності з специфікою та

особливостями діяльності організації (АС).

Відповідальність

Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов’язків, допущені ними порушення встановленого порядку захисту інформації в АС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

Персональна відповідальність керівника та співробітників СЗІ визначається посадовими (функціональними) інструкціями.

Відповідальність за діяльність СЗІ покладається на її керівника.

Керівник СЗІ відповідає за:

організацію робіт з захисту інформації в АС, ефективність захисту інформації відповідно до чинних нормативно-правових актів;

своєчасне розроблення і виконання “Плану захисту інформації в автоматизованій системі”;

якісне виконання співробітниками СЗІ завдань, функцій та обов'язків, зазначених у цьому Положенні, посадових інструкціях, а також планових заходів з захисту інформації, затверджених керівником організації;

координацію планів діяльності підрозділів та служб АС (організації) з питань захисту інформації;

створення системи навчання співробітників, користувачів, персоналу АС з питань захисту інформації;

виконання особисто та співробітниками СЗІ розпоряджень керівника організації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

Співробітники СЗІ відповідають за:

додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій;

повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в АС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції СЗІ;

дотримання термінів проведення контрольних, інспекційних, перевірочних та інших заходів з оцінки стану захищеності інформації в АС, які включені до плану робіт СЗІ;

якість та правомірність документального оформлення результатів робіт окремих етапів створення КСЗІ, документального оформлення результатів перевірок;

інші питання персональної відповідальності, які покладені на

керівника та співробітників СЗІ у відповідності з специфікою та особливостями діяльності АС (організації).

З метою визначення юридичного статусу СЗІ в установі, правового закріплення структури, завдань, функцій, повноважень СЗІ, а також організації її робіт із захисту інформації впродовж всього життєвого циклу ІКС в установі розробляється *“Положення про службу захисту інформації в ІКС установи”.*

Зміст *Положення* формується за такими розділами:
загальні положення;
завдання служби захисту інформації;
функції служби захисту інформації;
повноваження і відповідальність служби захисту інформації;
взаємодія служби захисту інформації з іншими підрозділами організації та зовнішніми підприємствами, установами, організаціями;
штатний розклад та структура служби захисту інформації;
організація робіт служби захисту інформації;
фінансування служби захисту інформації.

Залежно від конкретних завдань і умов функціонування служби захисту інформації дозволяється, у разі необхідності, поєднувати окремі розділи в один, вводити нові розділи (підрозділи) або вилучати розділи, що не є актуальними.

До Положення у вигляді додатків можуть включатися нормативні документи, таблиці, схеми, графіки, необхідні для визначення заходів захисту інформації, плани об’єктів захисту з вказівками робочих місць та встановлених на них технічних засобів передачі, прийому, зберігання, обробки інформації, що підлягає захисту та ін. документи.

Положення має бути погоджене з юрисконсультом та керівниками підрозділів (служби безпеки, РСО, підрозділу ТЗІ) організації.

Положення затверджується наказом керівника організації або підрозділу, до якого структурно входить СЗІ.

Зміни суттєвого характеру вносяться до Положення на основі розпорядження або наказу керівника організації (підрозділу, до якого структурно входить СЗІ).

Отже, служба захисту інформації – важливий структурний підрозділ установи, на який покладається велика кількість завдань, пов’язаних із розробкою, упровадженням, керуванням, модернізацією комплексною системою захисту інформації в ІКС, а також здійсненням контролю за її функціонуванням.

Тільки після створення СЗІ доцільно розпочинати роботи щодо

створення КСЗІ в ІКС.

Далі розглянемо загальний порядок проведення робіт із побудови КСЗІ в ІКС, покладених на СЗІ установи.

2.5.3 Етапи створення КСЗІ в ІКС та їхній нормативно-правовий супровід

Загальний порядок проведення робіт із побудови КСЗІ в ІКС регламентується положеннями основних Державних Стандартів України у сфері технічного захисту інформації ***ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення", ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт"*** *(їхній зміст було розглянуто раніше в цьому розділі).*

Щодо порядку проведення робіт зі створення КСЗІ в ІКС вимоги ДСТУ доповнюються положеннями нормативного документа ***НД ТЗІ 3.7-003-2023 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі", затвердженого наказом Адміністрації Держспецзв'язку від 28 жовтня 2023 року № 924.***

Цей нормативний документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-комунікаційних системах, порядок ухвалення рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІКС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу. [41]

НД ТЗІ не встановлює нових норм, а систематизує та деталізує в одному документі вимоги, норми й правила, які безпосередньо або опосередковано витікають з положень чинних стандартів та нормативних документів.

Цей НД ТЗІ побудовано у вигляді керівництва, яке містить перелік робіт і посилання на чинні нормативні документи, відповідно до яких ці роботи необхідно виконувати. Якщо якийсь з етапів чи видів робіт не нормовано, наводиться короткий зміст робіт та якими результатами вони повинні закінчуватись.

НД ТЗІ призначений для суб'єктів інформаційних відносин (власників або розпорядників ІКС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІКС, для постачальників компонентів ІКС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІКС яких обробляється інформація, яка є власністю держави, *належить до державної чи іншої таємниці* або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІКС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

Послідовність реалізації етапів та порядок проведення робіт кожного із етапів щодо створення КСЗІ в ІКС визначені в Розділі 6 – Етапи створення КСЗІ, а саме:

1 етап – Формування загальних вимог до КСЗІ в ІКС:

1.1 обґрунтування необхідності створення КСЗІ;

1.2 обстеження середовищ функціонування ІТС;

1.3 формування завдання на створення КСЗІ.

2 етап – Розробка політики безпеки інформації в ІКС:

2.1 вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт;

2.2 вибір варіанту КСЗІ;

2.3 оформлення політики безпеки.

3 етап – Розробка технічного завдання на створення КСЗІ:

3.1 вибір варіанта ТЗ (окремий розділ в ТЗ на створення ІКС; додаток до ТЗ на створення ІКС; окремий документ);

3.2 оформлення ТЗ

4 етап – Розробка проєкту КСЗІ:

4.1 ескізний проєкт (у разі необхідності);

4.2 технічний проєкт, робочий проєкт (або технороботчий проєкт), розробка документації на КСЗІ;

5 етап – Введення КСЗІ в дію та оцінка захищеності інформації в ІКС:

5.1 підготовка КСЗІ до введення в дію;

5.2 створення СЗІ установи;

5.3 доопрацювання документів Плану захисту інформації в ІКС;

5.4 навчання користувачів;

5.5 комплектування КСЗІ;

5.6 виконання будівельно-монтажних робіт, акт прийняття робіт;

5.7 виконання пусконалагоджувальних робіт (монтаж та атестація КТЗІ, встановлення, налагодження та перевірка працездатності КЗЗ, монтаж ОТЗ та ДТЗС, спецдослідження та інструментальні вимірювання рівня ПЕМВН, акт(и) виконаних робіт;

5.8 атестація КСЗІ.

5.9 проведення попередніх випробувань КСЗІ (затвердження програми та методики випробувань, проведення випробувань, складання Протоколу випробувань);

5.10 проведення дослідної експлуатації КСЗІ, акт результатів дослідної експлуатації;

5.11 проведення державної експертизи КСЗІ, акт державної експертизи;

6 етап – Супроводження КСЗІ

Із врахуванням накопиченого досвіду з моменту введення в дію НД ТЗІ 3.7-003-2023 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі”, затвердженого наказом Адміністрації Держспецзв’язку від 28 жовтня 2023 року № 924, до цього часу загальну послідовність створення КСЗІ в ІКС у достатньо деталізованому варіанті можна викласти так:

1 етап – Формування загальних вимог до КСЗІ в ІКС:

1.1 ***Обґрунтування необхідності створення КСЗІ в ІКС****:*

розробка концепції ІКС, визначення основних принципів та підходів до її побудови;
визначення завдань, характеристик, функціональних комплексів ІКС.

1.2 ***Створення СЗІ установи:***

видання наказу про створення СЗІ установи;
призначення осіб на посади в СЗІ;
затвердження "Положення про СЗІ установи".

1.3 ***Обстеження середовищ функціонування ІКС:***

призначення комісії з проведення обстеження та категоріювання ОІД установи (в/частини);

обстеження фізичного середовища функціонування ІКС:

визначення приміщень, в яких буде циркулювати ІзОД, складання актів категоріювання цих приміщень;
проведення організаційно-режимних заходів захисту визначених приміщень;
вирішення питань з електроживленням та заземленням ТЗПІ;
визначення засобів ТЗІ та КЗЗ;
відпрацювання актів відповідності визначених приміщень ступеню обмежування доступу до робіт, які в них будуть проводитись;

обстеження середовища користувачів ІКС;

обстеження обчислювальної системи, інформації та технології її обробки:

визначення характеристик ПЕОМ та ПЗ;
придбання, монтаж ПЕОМ, інсталяція ПЗ;
проведення категоріювання ПЕОМ;
відпрацювання акту (актів) обстеження середовищ функціонування ІКС.

1.4 ***Формування завдання на створення КСЗІ:***

визначення завдань захисту інформації в ІКС та мети створення КСЗІ;
розробка моделі загроз та моделі порушника;
здійснення аналізу ризиків втрати ІзОД;
визначення загальної структури та складу КСЗІ.

2етап – Розробка політики безпеки інформації в ІКС:

2.1 ***Вибір варіанту КСЗІ;***

2.2 ***Оформлення політики безпеки;***

2.3 ***Початок розробки Плану захисту інформації в ІКС****.*

3 етап – Розробка ТЗ на створення КСЗІ в ІКС, його затвердження та погодження:

3.1 ***Вибір варіанту технічного завдання****:*

- у вигляді окремого розділу в ТЗ на створення ІКС;
- у вигляді окремого (часткового) ТЗ;
- у вигляді доповнення до ТЗ на створення ІКС.

3.2 ***Оформлення технічного завдання та його погодження****.*

4 етап – Розробка проєкту КСЗІ:

3.3 ***Розробка ескізного проєкту*** (попередні проєктні рішення КСЗІ, розроблення, оформлення, узгодження та затвердження документації на КСЗІ);

4.2 ***Розробка технічного проєкту*** (загальні проєктні рішення щодо реалізації вимог ТЗ на КСЗІ, визначення організаційної структури та структури технічних і програмних засобів);

4.3 ***Розробка робочого проєкту*** (розроблення, оформлення та затвердження робочої та експлуатаційної документації КСЗІ).

5 етап – Введення КСЗІ в дію та оцінка захищеності інформації в ІКС:

5.1 ***Придбання засобів ТЗІ, КЗЗ, упровадження, монтаж та інсталяція; проведення робіт щодо реалізації заходів із захисту інформації від несанкціонованого витоку технічними каналами****;*

5.2 ***Проведення Атестації КТЗІ;***

5.3 ***Призначення відповідальних осіб****;*

5.4 ***Проведення навчання персоналу роботі з КЗЗ та забезпечення безпеки інформації на ОІД;***

5.5 ***Проведення попередніх випробувань КСЗІ в ІКС:***

організація та проведення Замовником та Розробником КСЗІ попередніх випробувань з метою перевірки працездатності КСЗІ згідно вимог ТЗ;
оформлення Протоколу випробувань з висновком щодо можливості прийняття КСЗІ у дослідну експлуатацію.

5.6 ***Дослідна експлуатації КСЗІ в ІКС:***

набуття практичних навичок всіма категоріями працівників з використання технічних та програмно-апаратних засобів захисту інформації;
засвоєння ними вимог нормативних та розпорядчих документів з питань забезпечення безпеки обробки інформації в ІКС;
відпрацювання технологій обробки інформації, розмежування доступу користувачів до ресурсів ІКС керування засобами захисту;
доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування КЗЗ, коригування робочої та експлуатаційної документації;
оформлення Акту про завершення *дослідної експлуатації з висновком щодо можливості представлення КСЗІ на державну експертизу.*

5.7 ***Проведення державної експертизи КСЗІ:***

подання КСЗІ в ІКС на державну експертизу;
визначення Організатора державної експертизи;
розробка, узгодження та затвердження програми та методики державної експертизи;
аналіз комплекту документів на КСЗІ в ІКС;
огляд об’єкта державної експертизи;
проведення експертних випробувань КСЗІ та оформлення результатів: протокол експертних випробувань на КСЗІ, експертний висновок;
розгляд матеріалів державної експертизи КСЗІ Експертною радою з питань ДЕ у сфері ТЗІ Адміністрації Держспецзв'язку;
отримання Атестату відповідності КСЗІ;
введення в експлуатацію ІКС із створеною КСЗІ.

6 етап – Супроводження КСЗІ:

обробка ІзОД в штатному режимі, планові роботи щодо підтримки належного стану захисту ІзОД, планові перевірки стану захищеності ІзОД.

Як бачимо, наведені вище етапи створення КСЗІ пов’язані із виконанням цілої низки взаємопов’язаних заходів. За цих обставин стає зрозумілою наявна чимала кількість НД ТЗІ, призначення та зміст яких спрямовані на надання допомоги посадовим особам СЗІ та іншим фахівцям, залученим до створення КСЗІ, щодо реалізації конкретних заходів, таких як: аналіз ризиків для інформації в ІКС, розробка моделі загроз та моделі порушника, формування політики безпеки інформації в ІКС, розробка технічного завдання на створення КСЗІ, розробка та виконання заходів Плану захисту інформації в ІКС та інші. Вимоги певної низки НД ТЗІ, зміст робіт кожного етапу створення КСЗІ та порядок їх виконання здобувачами вищої освіти докладно вивчаються на заняттях навчальних дисциплін “Технічний захист інформації”, “Системи та комплекси технічного захисту інформації”, “Убезпечення інформації від витоку технічними каналами”, “Побудова комплексних систем захисту інформації”.

2.6 Рекомендації щодо вивчення головних положень нормативно-правового забезпечення щодо системи безпеки інформації в ІКС, її моніторингу, аудиту та контролю виконання встановлених вимог

Головним завданням побудованої КСЗІ є забезпечення безпеки інформації в ІКС протягом усього її життєвого циклу. Реалізації цього головного завдання підпорядковується вся низка заходів, пов’язана із обґрунтуванням, створенням, атестацією та супроводженням КСЗІ в ІКС. Це завдання знаходить віддзеркалення у змісті всіх організаційно-розпорядчих та організаційно-технічних документів, які супроводжують відповідні етапи побудови та супроводження КСЗІ. Важливими складовими безпеки інформації в ІКС є також заходи моніторингу та аудиту системи безпеки інформації, а також організація та здійснення контролю виконання встановлених вимог безпеки інформації в ІКС.

Зміст головних складових безпеки інформації в ІКС доцільно з’ясувати під час групових (практичних) занять за розглянутою раніше методикою (а також під час самостійної роботи здобувачів вищої освіти) шляхом вивчення положень відповідних нормативних документів у послідовності, що наведена нижче.

2.6.1 Порядок розробки та реалізації положень Політики безпеки інформації в ІКС

Одним із найважливіших документів, спрямованих на захист інформації від певних загроз, є *Політика безпеки інформації в ІКС (далі – Політика безпеки)*.

Політика безпеки інформації в ІКС це документ, що містить набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Термін "політика безпеки" може бути застосований щодо ІКС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в ІКС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи.

Основні положення щодо розробки змісту та шляхів реалізації Політики безпеки інформації в ІКС визначені у *Розділі 5 Додатку до* ***НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".***

Обсяг завдань щодо роботи з положеннями Додатку до НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі":

– опрацювати Розділ 5 Додатку НД ТЗІ у повному обсязі;

– особливу увагу під час роботи звернути на положення п.п. 5.5 – 5.7.

Контрольні питання:

1. *Що таке Політики безпеки інформації в ІКС (п. 5.1)?*
2. *Які чинники повинна враховувати Політика безпеки (п. 5.2)?*
3. *На яких принципах повинна базуватись Політика безпеки (п. 5.4)?*
4. *Які гарантії повинна доказово надавати Політика безпеки (п. 5.5)?*
5. *Які роботи включає в себе методологія розроблення Політики безпеки (п. 5.6)?*
6. *Яке місце в Політиці безпеки займають правила розмежування доступу (ПРД) користувачів до інформації та в які способи вони можуть бути реалізовані (п.п. 5.7, 5.7.1)?*

Отже, *Політика безпеки інформації в ІКС є одним із головних документів, призначених для забезпечення безпеки інформації в ІКС протягом увсього її життєвого циклу.*

2.6.2 Порядок розробки та виконання Плану захисту інформації в ІКС

План захисту інформації в ІКС (далі – План захисту) є сукупністю документів, згідно з якими здійснюється організація захисту інформації на всіх етапах життєвого циклу ІКС.

В окремих випадках План захисту інформації в ІКС може оформлятися одним документом *(надати пояснення здобувачам вищої*

освіти).

Основні положення щодо обсягу та змісту Плану захисту інформації в ІКС визначені у *Методичних вказівках щодо структури та змісту Плану захисту інформації в автоматизованій системі Додатку до* ***НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі".***

Обсяг завдань щодо роботи з положеннями *Методичних вказівок щодо структури та змісту Плану захисту інформації в автоматизованій системі Додатку до НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі"*:

– опрацювати *Методичні вказівки* Додатку НД ТЗІ у повному обсязі.

Контрольні питання:

1. Що таке План захисту інформації в автоматизованій системі?
2. На підставі яких даних розробляється План захисту?
3. Які положення повинні бути документально закріплені у Плані захисту?
4. З яких розділів (окремих документів) складається План захисту?

Отже, План захисту є обов'язковим документом для АС, в яких обробляється інформація, що становить державну або іншу встановлену законом таємницю, службова інформація, інформація, яка належить до державних інформаційних ресурсів, або інформація, необхідність захисту якої встановлено законом.

2.6.3 Порядок організації та здійснення аудиту та моніторингу системи безпеки інформації в ІКС

Важливими складовими безпеки інформації в ІКС є заходи *аудиту та моніторингу системи безпеки інформації*.

Аудит інформаційної безпеки *– це системний процес одержання об'єктивних якісних і кількісних оцінок про поточний стан безпеки інформації в ІКС установи у відповідності з визначеними критеріями та показниками безпеки.*

Аудит дозволяє оцінити поточну безпеку функціонування ІКС, оцінити й прогнозувати ризики, керувати їхнім впливом на процеси управлінської діяльності установи, коректно й обґрунтовано підійти до питання забезпечення безпеки її інформаційних ресурсів, вмісту корпоративних баз даних, стратегічних планів розвитку, поточних програм функціонування, фінансових, бухгалтерських відомостей тощо.

Основні напрямки діяльності в області аудиту безпеки інформації деталізуються на такі: атестацію; контроль захищеності інформації; спеціальні дослідження технічних засобів і проєктування об'єктів в захищеному виконанні.

Атестація об'єктів інформатизації за вимогами безпеки інформації:

атестація автоматизованих систем, засобів зв'язку, обробки і передачі інформації;

атестація приміщень, призначених для ведення конфіденційних переговорів;

атестація технічних засобів, встановлених у виділених приміщеннях.

Контроль захищеності інформації обмеженого доступу:

виявлення технічних каналів витоку інформації та шляхів несанкціонованого доступу до неї;

контроль ефективності застосовуваних засобів захисту інформації.

Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань і наведень (ПЕМВН):

персональні ЕОМ, засоби зв'язку та обробки інформації;

локальні обчислювальні системи;

оформлення результатів досліджень у відповідності з встановленими вимогами.

Проєктування об'єктів в захищеному виконанні:

розробка концепції інформаційної безпеки;

проєктування автоматизованих систем, засобів зв'язку, обробки і передачі інформації в захищеному виконанні;

проєктування приміщень, призначених для ведення конфіденційних переговорів.

Види і цілі аудиту

Аудит інформаційної безпеки поділяється на *зовнішній* та *внутрішній*.

Зовнішній аудит – це, як правило, одноразовий захід, що проводиться за ініціативою керівництва установи. Зовнішній аудит є незалежним і його результати максимально об’єктивні.

Внутрішній аудит – це безперервна діяльність, яка здійснюється підрозділом внутрішнього аудиту (СЗІ).

Цілями проведення аудиту безпеки є:

аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки у відношенні до ресурсів ІС;

оцінка поточного рівня захищеності ІС;

локалізація вузьких місць у системі захисту ІС;

оцінка відповідності ІС існуючим стандартам в галузі інформаційної безпеки;

вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІКС.

До кола додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

розробка (коригування) політики безпеки та інших організаційно-розпорядчих документів із захисту інформації та участь у їх упровадженні в роботу організації;

постановка (уточнення) завдань для ІТ-персоналу, що стосуються забезпечення захисту інформації;

участь у навчанні користувачів і обслуговуючого персоналу ІКС з питань забезпечення інформаційної безпеки;

участь у розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

інші завдання.

Внутрішній аудит передбачає застосування технологій *активного аудиту* (друга назва – технології активного управління безпекою в ІКС), завдання яких полягає у виявленні загрози безпеці інформації та в режимі реального часу адекватного реагування на їх усунення.

Технології активного аудиту містять у собі такі компоненти:

засоби виявлення й аналізу атак;

засоби аналізу захищеності й пошуку уразливості об’єктів ІКС (робочі станції, сервери, СУБД, мережеві з’єднання тощо);

засоби адаптації й керування налаштуваннями засобів захисту в режимі реального часу при зміні інфраструктури або атаках.

Засоби аналізу захищеності й виявлення атак виконують функції моніторингу безпеки ІКС.

Засоби аналізу захищеності досліджують налаштування елементів захисту ОС на робочих станціях і серверах, базах даних. Вони аналізують топологію мережі, шукають незахищені або неправильні мережні з’єднання, аналізують налаштування міжмережних екранів. Засоби аналізу захищеності за принципом їхньої роботи називають також *сканерами безпеки*. Якщо сканер містить засоби керування налаштуваннями засобів безпеки, то він може виконати їхню переконфігурацію самостійно.

Наявність сканерів безпеки в арсеналі адміністратора безпеки дозволяє значно знизити ризик наявності невиявлених загроз і рятує його

від кропіткого та довгого аналізу та відповідної конфігурації налаштувань безпеки й мережних налаштувань вручну.

Методика активного аудиту має назву ***моніторинг безпеки інформації в ІКС.***

Із наведеного вище стають зрозумілими цілі, завдання, механізми реалізації та важливість аудиту та моніторингу системи безпеки інформації в ІС.

Мета, завдання та порядок проведення постійного моніторингу безпеки інформації в ІКС визначені у положеннях ***НД ТЗІ 3.6-008-21 "Порядок моніторингу безпеки інформаційних систем".***

Цей НД ТЗІ визначає порядок проведення постійного моніторингу безпеки інформаційних систем (ІС) як окремий етап Порядку впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах

Постійний моніторинг безпеки інформаційних систем є одним з етапів життєвого циклу системи безпеки інформації в Організації. [46]

Обсяг завдань щодо роботи з положеннями *НД ТЗІ 3.6-008-21 "Порядок моніторингу безпеки інформаційних систем"*:

– опрацювати зміст НД ТЗІ у повному обсязі.

Контрольні питання та завдання:

1. *Яка мета етапу моніторингу безпеки інформації в ІКС (п. 5.1)?*
2. *Доповісти про опис завдань та очікуваних результатів постійного моніторингу безпеки (таблиця 5.1).*
3. *На якому рівні та в якому порядку проводиться постійний моніторинг безпеки інформації в ІКС (п. 5.2, рисунок 5.2)?*
4. *Які складові системи безпеки інформації формуються в результаті постійного моніторингу безпеки (п. 5.2)?*
5. *Які основні задачі проведення аналізу ризиків на системному рівні (п. 5.3)?*

У переліку заходів щодо організації технічного захисту інформації поряд зі здійсненням моніторингу та аудиту системи безпеки інформації в ІС особливе місце займає здійснення державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації.

2.6.4 Організація та здійснення контролю виконання встановлених вимог безпеки інформації в ІКС

Порядок організації та здійснення контролю виконання встановлених вимог безпеки інформації в ІКС визначено у положеннях *"Порядку здійснення державного контролю за станом технічного захисту*

державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури" (затверджений наказом Адміністрації Держспецзв'язку від 08 квітня 2021 року *№ 61/ДСК).* [47]

Діяльність щодо здійснення державного контролю за станом технічного захисту інформації в інформаційно-телекомунікаційних системах в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України та миротворчих контингентах України за кордоном безпосередньо покладається на Департамент державного контролю за станом криптографічного та технічного захисту інформації.

За результатами цієї діяльності готуються та подаються на розгляд Президентові України, Голові Верховної Ради України і Прем'єр-міністрові України рекомендації щодо поліпшення стану захисту інформації в державі. Впровадження цих рекомендацій дозволяє підтримувати стан захищеності інформації та інформаційних ресурсів держави на належному рівні.

Державний контроль за станом ТЗІ полягає в перевірці виконання вимог нормативно-правових актів і нормативних документів з ТЗІ та здійснюється з метою визначення стану ТЗІ в органах, щодо яких здійснюється ТЗІ, виявлення порушень з ТЗІ та запобігання їм.

Обсяг завдань щодо роботи з положеннями *"Порядку здійснення державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури" (затверджений наказом Адміністрації Держспецзв'язку від 08 квітня 2021 року № 61/ДСК):*

– опрацювати зміст НПА у повному обсязі.

Контрольні питання та завдання:

1. *Яким шляхом здійснюється державний контроль за станом ТЗІ Держспецзв'язку?*
2. *Які заходи містить контрольно-інспекторська робота з питань ТЗІ?*
3. *Доповісти про види перевірок стану ТЗІ, їх завдання та періодичність проведення.*
4. *Що є підставами для здійснення планових перевірок стану ТЗІ в установах?*

5. *Що є підставами для здійснення позапланових перевірок стану ТЗІ в установах?*
6. *Доповісти про види перевірок стану ТЗІ, їх завдання та періодичність проведення.*
7. *Чи зобов'язана Адміністрації Держспецзв'язку сповіщати установи щодо здійснення в них перевірок стану ТЗІ?*
8. *Які категорії посадових осіб залучаються до здійснення державного контролю стану ТЗІ в установах?*
9. *Які документи є підставою для допуску посадових осіб, які прибули для перевірки стану ТЗІ в установі?*
10. *Які повноважень мають посадові особи, які прибули для перевірки стану ТЗІ в установі?*
11. *Який порядок документування результатів перевірки стану ТЗІ в установі?*
12. *Які варіанти висновків стану ТЗІ у перевіреній установі можуть бути вказані у Акті перевірки?*
13. *Яких подальших дій вимагають кожний із можливих висновків стану ТЗІ у перевіреній установі?*
14. *Доповісти про порядок відновлення інформаційної діяльності на відповідних об'єктах установи у разі її припинення за результатами виявлених порушень в ході перевірок стану ТЗІ.*

Отже, кожний із вище розглянутих нормативних документів, що містять вимоги до системи безпеки інформації в ІС, визначають порядок її моніторингу, аудиту та контролю виконання встановлених вимог, займає своє важливе місце в загальній системі нормативно-правового забезпечення безпеки інформації під час її обробки в ІКС.

2.7 Державна експертиза у сфері технічного захисту інформації

2.7.1 Методичні рекомендації щодо вивчення головних положень нормативно-правового забезпечення стосовно організації та порядку проведення робіт з державної експертизи у сфері ТЗІ

Із матеріалу попередніх глав даного розділу відомо, що у разі, коли на ОІД установи створюється КТЗІ або КСЗІ в ІКС на етапах їхнього упровадження, як правило, використовуються технічні засоби, *які за встановленим порядком пройшли державну експертизу та мають експертний висновок щодо можливостей їхнього використання на ОІД відповідних категорій, державна експертиза здійснюється щодо організаційно-технічних рішень для впровадження типової компоненти КСЗІ в ІКС, а також самої КСЗІ на заключному етапі її створення. До проведення заходів державної експертизи у сфері ТЗІ мають безпосереднє відношення певні структурні підрозділи ДССЗЗІ України.*

З огляду на те, що після випуску з інституту здобувачів вищої освіти, ці завдання можуть стати частиною їхніх службових обов'язків на відповідних посадах, доцільно на заняттях з освітнього компонента "Нормативно-правове забезпечення інформаційної безпеки" розглянути вимоги чинних НПА щодо порядку проведення робіт з державної експертизи у сфері технічного захисту інформації. З цією метою у змісті робочої програми цього освітнього компонента доцільно передбачити проведення відповідного групового (практичного) заняття.

На цьому груповому (практичному) занятті за раніше розглянутою методикою в главі 1.3 розділу 1 посібника послідовно вивчаються вимоги *"Положення про державну експертизу в сфері технічного захисту інформації" (затверджено наказ Адміністрації Держспецзв'язку від 16 травня 2007 року № 93, зареєстровано в Міністерстві юстиції України 16 липня 2007року за № 820/14087) та НД ТЗІ 2.6-001-11 "Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах" (затверджено наказом Адміністрації Держспецзв'язку від 25 березня 2011 року № 65) (НД ТЗІ 2.6-001-11).* [48, 49]

Обсяг завдань щодо роботи з ***"Положенням про державну експертизу в сфері технічного захисту інформації", затвердженого наказом Адміністрації Держспецзв'язку від 16 травня 2007 року № 93, зареєстрованого в Міністерстві юстиції України 16 липня 2007 року за № 820/14087:***

– опрацювати Розділ 1 у повному обсязі, Розділ ІІ ст. ст. 1 – 16 включно.

Контрольні питання та завдання:

1. *Яка мета державної експертизи в сфері ТЗІ (Розділ 1 ст. 2)?*
2. *Навести перелік суб'єктів експертизи (Розділ 1 ст. 3).*
3. *Що є об'єктами державної експертизи (Розділ 1 ст. 4)?*
4. *У який спосіб може проводитись державна експертиза (Розділ 1 ст. 5)?*
5. *У яких випадках експертиза проводиться шляхом аналізу декларацій (Розділ 1 ст. 6)?*
6. *У яких випадках експертиза проводиться шляхом експертних випробувань (Розділ 1 ст. 6 останній абзац)?*
7. *Доповісти про види державної експертизи та умови (обставини) їх проведення (Розділ 1 ст. 7).*
8. *Які функції покладені на Адміністрацію Держспецзв'язку щодо організації та проведення експертизи (Розділ 1 ст. 8)?*
9. *Які функції покладені на територіальні органи Адміністрації Держспецзв'язку щодо організації та проведення експертизи (Розділ 1 ст.ст. 9, 10)?*
10. *Який орган створений в Адміністрації Держспецзв'язку з метою організації та проведення експертиз (Розділ ІІ ст. 1)?*
11. *Які органи створюються в територіальних органах Адміністрації Держспецзв'язку з метою організації та проведення експертиз шляхом аналізу декларації (Розділ ІІ ст. 2)?*
12. *Доповісти про порядок проведення експертизи КСЗІ шляхом експертних випробувань (Розділ ІІ ст. ст. 3, 4).*
13. *Який гранично максимальний термін дії зареєстрованої декларації (Розділ ІІ ст. 7)?*

Отже, *"Положення про державну експертизу в сфері технічного захисту інформації" (затверджено наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087) є одним із головних документів, що визначають в державі загальний порядок проведення державної експертизи у сфері технічного захисту інформації.*

Другим базовим НПА в цьому секторі ІБ є ***НД ТЗІ 2.6-001-11 "Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах", затверджено наказом Адміністрації Держспецзв'язку від 25***

березня 2011 року № 65, *який встановлює обсяг та порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу (НСД) та комплексних систем захисту інформації (КСЗІ).*

НД призначено для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, а також підприємств, установ і організацій всіх форм власності, які виконують роботи зі створення та проведення експертизи засобів технічного захисту інформації (ЗТЗІ) від НСД та КСЗІ в ІТС на відповідність вимогам НД системи ТЗІ в Україні.

В контексті розгляду послідовності створення *комплексних систем захисту інформації в ІКС* під час роботи з даним нормативним документом більше уваги доцільно приділити вивченню відповідних розділів, положення яких стосуються саме цих питань.

Обсяг завдань щодо роботи з ***НД ТЗІ 2.6-001-11 "Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах", затверджено наказом Адміністрації Держспецзв'язку від 25 березня 2011 року № 65:***

– ознайомитись із структурою побудови та назвами розділів змісту НД ТЗІ;

– опрацювати *розділ 7 Опис порядку проведення робіт з експертизи комплексних систем захисту інформації* НД ТЗІ у повному обсязі.

Контрольні питання:

1. *Який перелік робіт містить первинна експертиза КСЗІ (п. 7.1.1)?*
2. *Доповісти про мету та перелік дій кожного із видів робіт первинної експертизи об'єктів (п. 7.1.1.1)?*
3. *Виконання яких експертних робіт передбачає проведення експертних випробувань та досліджень об'єкта експертизи (п. 7.1.1.5.1)?*
4. *У чому полягають особливості проведення робіт з додаткової та контрольної експертизи КСЗІ (п. 7.2.1)?*
5. *Порівняйте ступінь деталізації порядку виконання заходів державної експертизи, наведених у попередньому НПА та даному нормативному документі, сформулюйте свою думку з цього приводу.*

Отже, положеннями НД ТЗІ 2.6-001-11 "Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах", затверджено наказом Адміністрації Держспецзв'язку від 25 березня 2011 року № 65, не тільки

встановлено обсяг робіт державної експертизи, а й детально та покроково (майже як в інструкції) визначений порядок їх реалізації. Даний документ є дуже важливим та корисним під час практичного виконання будь яких робіт державної атестації відповідними фахівцями.

2.7.2 Встановлений нормативними документами порядок проведення експертних робіт у сфері ТЗІ

Вивчення та узагальнення положень вище наведених НПА надає можливість сформувати у здобувачів вищої освіти необхідні фахові знання та компетентності. З метою перевірки правильності розуміння здобувачами вивчених положень даних НПА викладачу доцільно у переліку питань для проведення заходів поточного контролю передбачити й *питання щодо мети та послідовності проведення експертних робіт у сфері ТЗІ в державі (на прикладі державної експертизи КСЗІ)*.

Відповіді здобувачів повинні бути максимально наближеними до нижче сформульованих положень. [48, 49]

Державна експертиза у сфері технічного захисту інформації проводиться з *метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення ТЗІ.*

Об'єктами експертизи є:

комплексні системи захисту інформації, які є невід'ємною складовою ІКС;

апаратні, апаратно-програмні і програмні засоби, які реалізують функції ТЗІ або оцінки стану захисту інформації (далі – засоби ТЗІ);

організаційно-технічні рішення для впровадження типової компоненти КСЗІ в ІКС (типове ТЗ, організаційно технічні рішення КСЗІ тощо).

Експертиза може бути *первинною, додатковою та контрольною*.

Первинна експертиза є основним видом експертизи і передбачає виконання Організатором заходів, визначених у розділі ІІ цього Положення, для підготовки та ухвалення рішення щодо об'єкта експертизи.

Додаткова експертиза проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини, а також у зв'язку із закінченням строку дії документів, що засвідчують результати експертизи.

Контрольну експертизу проводить інший Організатор з ініціативи Замовника у разі наявності у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації Держспецзв'язку для перевірки висновку первинної чи додаткової експертизи.

Порядок проведення державної експертизи КСЗІ в ІКС.

Державна експертиза КСЗІ ІКС, може здійснюватися:
шляхом експертних випробувань;
шляхом аналізу поданих установами декларації.

З метою організації та проведення експертиз, координації заходів і ухвалення рішень щодо проведення експертиз в Адміністрації Держспецзв'язку створена *експертна рада з питань державної експертизи в сфері технічного захисту інформації (далі – Експертна рада).*

З метою проведення експертизи КСЗІ в ІКС шляхом аналізу декларації в територіальних органах Адміністрації Держспецзв'язку створені *експертні комісії з питань державної експертизи в сфері технічного захисту інформації (далі – Експертна комісія).*

Порядок проведення експертизи шляхом експертних випробувань.

Для проведення експертизи *шляхом експертних випробувань* Замовник надсилає на ім'я Голови Держспецзв'язку (крім випадків, передбачених розділом IV "Положення про державну експертизу в сфері технічного захисту інформації") *заяву* про проведення первинної / додаткової / контрольної експертизи КСЗІ в ІКС встановленої форми.

За результатами розгляду заяви Експертна рада Держспецзв'язку ухвалює рішення про доцільність проведення експертизи та визначає її Організатора з урахуванням пропозиції Замовника.

Про рішення Експертної ради Замовнику та Організатору надсилається письмове повідомлення.

Основним документом, що регламентує відносини між Замовником і Організатором, є укладений між ними *договір на проведення експертизи*.

Замовник надає Організатору комплект технічної документації на об'єкт експертизи, необхідної для проведення експертних випробувань.

Організатор за результатами аналізу наданих документів та з урахуванням загальних методик оцінювання задекларованих характеристик засобів ТЗІ, ОТР КСЗІ та КСЗІ формує *програму і методику проведення експертизи об'єкта*, *здійснює відбір зразків засобів ТЗІ та складає перелік необхідного програмно-технічного забезпечення для проведення випробувань.*

Програма проведення експертизи погоджується із Замовником. Програма та методика проведення експертизи апаратних, апаратно-програмних засобів ТЗІ, які реалізують функції щодо захисту інформації від витоку технічними каналами, погоджуються із Замовником та Адміністрацією Держспецзв'язку.

В терміни, визначені у Договорі, *Експерти* здійснюють заходи державної експертизи на об'єкті експертизи *Замовника* відповідно до затверджених програми та методики.

Результати роботи Експертів оформлюються у вигляді *протоколу виконання експертних робіт,* який надається на розгляд *Організатору ДЕ.*

Результати робіт, визначених методикою, узагальнює Організатор в *Експертному висновку.* У разі позитивних результатів експертної оцінки Організатор складає *атестат відповідності на КСЗІ.*

Зазначені документи, що підтверджують відповідність вимогам нормативних документів з ТЗІ, засвідчує Організатор і разом з програмою, методикою та протоколами виконання робіт подає для розгляду до *Адміністрації Держспецзв'язку.*

У разі позитивного рішення документи реєструються в Адміністрації Держспецзв'язку, атестат відповідності на КСЗІ ІКС передається Замовнику.

Отримання Замовником атестату відповідності на КСЗІ є підставою для введення в експлуатацію ІКС.

Строк дії атестата відповідності КСЗІ визначає Організатор:

для атестата відповідності КСЗІ автоматизованої системи класу 1 – безстроковий;

для атестата відповідності КСЗІ автоматизованої системи класів 2, 3 – до 5 років.

Порядок проведення експертизи шляхом аналізу декларації

Для проведення експертизи КСЗІ в ІКС <u>*шляхом аналізу декларації*</u> Замовник надсилає декларацію про відповідність КСЗІ вимогам нормативних документів з ТЗІ згідно з *додатком 4 до Положення*, формуляр ІКС, акт про завершення робіт зі створення КСЗІ:

до Адміністрації Держспецзв'язку – на ім'я Голови Держспецзв'язку для ІКС, які розташовано за територіальною ознакою у місті Києві і Київській області;

до відповідного територіального органу Адміністрації Держспецзв'язку – на ім'я керівника територіального органу Держспецзв'язку за місцезнаходженням ІКС.

За результатами аналізу декларації і поданих разом із нею документів Експертна рада (Експертна комісія) ухвалює рішення про реєстрацію декларації. Зареєстровану декларацію та інші подані документи

Адміністрація Держспецзв'язку (її територіальний орган) повертає Замовнику.

У разі неподання разом із декларацією документів, зазначених у пункті 3 розділу ІІ *Положення*, неповноти наданих у них відомостей або невідповідності порядку створення КСЗІ вимогам нормативних документів з ТЗІ, недостатності чи некоректності обраних методів оцінки механізмів захисту інформації відповідно до вимог нормативних документів з ТЗІ Адміністрація Держспецзв'язку (територіальний орган Адміністрації Держспецзв'язку) письмово повідомляє Замовника про відмову в реєстрації декларації, причини, через які реєстрація не є можливою, та повертає декларацію і подані з нею документи на доопрацювання або ухвалює рішення про ознайомлення з фактичним станом об'єкта експертизи для визначення відповідності наданим документам, а також письмово повідомляє Замовника про прийняте рішення.

Після усунення причин, що стали підставою для відмови у реєстрації декларації, Замовник надсилає для повторного розгляду до Адміністрації Держспецзв'язку (територіального органу Адміністрації Держспецзв'язку) доопрацьовану декларацію і документи, які подаються разом з нею.

Зареєстрована декларація або атестат відповідності КСЗІ скасовується Адміністрацією Держспецзв'язку в разі внесення змін до КСЗІ, не передбачених техноробочим проєктом на КСЗІ, та/або порушення вимог з експлуатації КСЗІ.

Термін дії зареєстрованої декларації є необмеженим, крім декларацій на КСЗІ в ІКС, які створено на основі ОТР КСЗІ, строк дії якої встановлюється вимогами ОТР КСЗІ (але не більше ніж 5 років).

Документи, що розробляються під час організації та проведення державної експертизи

Проведення державної експертизи пов'язане із відпрацюванням цілої низки документів як Замовником експертизи, так і іншими суб'єктами (Організатором, Експертом та іншими).

На підставі вимог нормативних документів сформуємо перелік основних документів, які відпрацьовуються суб'єктами державної експертизи в процесі її проведення.

Замовником державної експертизи відпрацьовуються та за встановленим порядком подаються:

заява про проведення експертизи КСЗІ згідно з *додатком 1 Положення* (до якої додається ТЗ на створення КСЗІ);

або ***декларація про відповідність КСЗІ вимогам нормативних документів з ТЗІ*** згідно *з додатком 4 Положення* (до якої додаються; формуляр ІКС, акт про завершення робіт зі створення КСЗІ);

Організатор державної експертизи відпрацьовує:

договір на проведення державної експертизи (разом із Замовником);

програму та методику проведення експертизи об'єкта експертизи (погоджені із Замовником та Адміністрацією Держспецзв'язку);

експертний висновок згідно з *додатком 6 Положення;*

атестат відповідності на КСЗІ згідно *з додатком 7 Положення*;

Експерт відпрацьовує:

протокол(и) виконання робіт згідно *з додатком 5 Положення;*

Адміністрацією Держспецзв'язку (територіальним органом Адміністрації Держспецзв'язку) можуть бути відпрацьовані:

рішення Експертної ради Адміністрації Держспецзв'язку про доцільність проведення експертизи;

рішення про реєстрацію декларації;

лист-відмова у реєстрації декларації *(у разі зауважень до якості та встановленого обсягу поданих документів на експертизу);*

припис на право ознайомлення з фактичним станом об'єкта експертизи *згідно з додатком 11 Положення****;***

звіт за результатами ознайомлення з фактичним станом об'єкта експертизи *згідно з додатком 12 Положення*;

рішення про зупинення дії експертного висновку та/або атестата відповідності КСЗІ.

Отже, державна експертиза КСЗІ є важливим процесом дослідження, перевірки, аналізу та оцінки об'єкта експертизи щодо його відповідності вимогам нормативних документів з технічного захисту інформації та можливості використання для забезпечення ТЗІ із обов'язковим документуванням (тобто юридичним оформленням) кожного етапу експертизи.

Висновки до розділу 2

У змісті пунктів розділу 2 розглянуто напрямки нормативно-правового забезпечення у сфері технічного захисту інформації в цілому, а також щодо забезпечення захисту інформації в інформаційних та інформаційно-комунікаційних системах зокрема.

Положеннями чинних державних стандартів та НПА у сфері ТЗІ встановлені визначення основних термінів та понять, які використовуються в різних сферах діяльності установ, змістом яких є обробка інформації з використанням інформаційних (автоматизованих) систем. Встановлена термінологія надає можливість формулювати вимоги чинних НПА в сфері ТЗІ, а також забезпечує єдиноправильне розуміння суті викладених вимог всіма суб'єктами інформаційних відносин.

Розглянуті у розділі положення цілої низки нормативно-правових актів та нормативних документів, чинних у сфері ТЗІ, надають розуміння обґрунтованого на юридичному рівні порядку упровадження організаційних, організаційно-технічних, програмно-апаратних (програмних) заходів захисту інформації, яка є власністю держави, у разі її обробки засобами автоматизації.

Так, "Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" (постанова КМУ від 18 грудня 2013 року № 373, зі змінами), встановлені загальні вимоги до системи забезпечення безпеки державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, під час їх обробки в інформаційних та інформаційно-комунікаційних системах установ.

Положеннями НД ТЗІ 3.6-004-21 "Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці" визначені основи організації та порядок впровадження системи безпеки інформації (СБІ) в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

Система безпеки інформації різного ступеня критичності (на об'єктах відповідної категорії) повинна передбачати й відповідні переліки заходів та засобів захисту. Чим вищий рівень критичності оброблюваної в ІКС інформації, тим вищі вимоги щодо гарантій безпеки інформації, які повинні забезпечити впроваджені заходи та засоби захисту.

В ІКС, в яких обробляється інформація, що складає державну таємницю, повинна бути створена комплексна система захисту інформації.

Важливими чинниками ухвалення правильних рішень щодо побудови системи захисту інформації в ІКС є приналежність їх до певної категорії та класу.

Категорія об'єкта (ІКС) є важливою класифікаційною характеристикою важливості об'єкта, за якою визначається необхідний рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об'єкті. Категорія об'єкта суттєво впливає на склад

комплексу засобів захисту інформації та інших організаційно-технічних заходів, які необхідно впроваджувати на об'єктах інформаційної діяльності.

НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", а також НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу", встановлюють критерії оцінки захищеності інформації, оброблюваної в ІКС, від несанкціонованого доступу, надають рекомендації для визначення необхідного функціонального профілю захищеності інформації в конкретній ІКС, складають нормативно-методологічну базу для розроблення та впровадження комплексів засобів захисту інформації, яка обробляється в ІКС, та створення комплексних систем захисту інформації в них.

Положеннями ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення", ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт", НД ТЗІ 3.7-003-2023 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі" визначаються основи організації та порядок виконання робіт із захисту інформації в інформаційно-комунікаційних системах, порядок ухвалення рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІКС і видів інформації, яка в них оброблюється, визначення обсягу, змісту, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Важливим етапом створення та подальшого супроводження комплексної системи захисту інформації в ІКС є створення та організація роботи Служби захисту інформації установи у повній відповідності до вимог НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі", (затверджене наказом ДСТСЗІ СБ України від 04.12.2000 № 53). Тільки фахівці-посадові особи СЗІ установи здатні забезпечити своєчасне, якісне вирішення багатоетапних та багатопланових завдань щодо створення КСЗІ в ІКС, розпочинаючи з формування загальних вимог до КСЗІ в ІКС на першому етапі до проведення державної експертизи КСЗІ на останньому, а також супроводження КСЗІ надалі.

Нормативні документи у сфері ТЗІ "Положення про державну експертизу в сфері технічного захисту інформації" (наказ Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087), а також НД ТЗІ 2.6-001-11 "Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах"

встановлюють обсяг та порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу (НСД) та комплексних систем захисту інформації (КСЗІ). Знання положень даних нормативних документів є дуже важливими та корисними під час практичного виконання будь яких робіт державної експертизи відповідними фахівцями.

Огляд переліку, призначення та змісту головних законодавчих та НПА України у цьому розділі посібника надає здобувачам вищої освіти певну модель системного накопичення необхідних професійних знань у подальшому вивченні положень чималої кількості чинних нормативних документів держави в цій сфері.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ (ПРОВЕДЕННЯ ПОТОЧНОГО КОНТРОЛЮ)

1. Доповісти про призначення та спрямованість змісту Державного стандарту України 2226-93.
2. Відповідно до положень Державного стандарту України 2226-93 надати визначення термінам *“система автоматизована (АС)” “інформаційна (автоматизована) система”, “інформаційно-комунікаційна система”*. Надайте пояснення, наведіть приклади.
4. Доповісти про призначення та спрямованість змісту НПА “Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” (постанова КМУ від 29 березня 2006 року № 373, зі змінами).
5. Які категорії інформації підлягають обов'язковому захисту (відповідно до положень постанови КМУ від 29 березня 2006 року № 373, зі змінами)?
6. Відповідно до положень постанови КМУ від 29 березня 2006 року № 373, зі змінами, надати визначення терміну *“комплексна система захисту інформації”* (далі – КСЗІ) в ІКС. Доповісти про призначена КСЗІ.
7. Доповісти про призначення та спрямованість змісту НПА “Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці” (НД ТЗІ 3.6-004-21).
8. Відповідно до положень НД ТЗІ 3.6-004-21 навести категорії інформації за типом властивостей, що забезпечуються.
9. Навести категорії інформаційно-комунікаційних систем та ОІД, на яких вони розміщені. Навести приклади ІКС кожної категорії.

10. Доповісти призначення та спрямованість змісту НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.

11. Відповідно до положень НД ТЗІ 2.5-005-99 навести класи АС. Надати пояснення, що означає скорочена абревіатура: *АС «1.КД»*?

12. Доповісти про призначення та спрямованість змісту НД ТЗІ 2.5-008-2002 “Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2”.

13. Відповідно до положень НД ТЗІ 2.5-008-2002 надати пояснення, що таке несанкціонований доступ (НСД) до інформації, яка обробляється в АС? Які можливі способи реалізації зловмисниками НСД до інформації в АС?

14. На які групи розбиті критерії безпеки інформації, яка обробляється в АС (відповідно до положень НД ТЗІ 2.5-004-99)?

15. Надати визначення терміну *“витік інформації”*.

16. На які групи можна розподілити канали витоку інформації за фізичною природою їхнього походження?

17. Доповісти про призначення та спрямованість положень ДСТУ 3396.0-96, ДСТУ 3396.1-96.

18. Доповісти про призначення та спрямованість положень:

“Концепції технічного захисту інформації в Україні”, введеної в дію постановою КМУ від 8 жовтня 1997 року № 1126;

“Положення про технічний захист інформації в Україні”, введеного в дію указом Президента України від 27 вересня 1999 року № 1229/99;

НД ТЗІ 1.4-001-2000 “Типове положення про службу захисту інформації в автоматизованій системі”;

НД ТЗІ 3.7-003-2023 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі”, затвердженого наказом Адміністрації Держспецзв’язку від 28 жовтня 2023 року № 924.

19. На підставі положень чинних НПА та нормативних документів у сфері ТЗІ обґрунтувати необхідність створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності установ.

20. Надати визначення терміну *“система ТЗІ”* (відповідно до положень “Концепції технічного захисту інформації в Україні”, введеної в дію постановою КМУ від 8 жовтня 1997 року № 1126.

21. Надати визначення терміну *“комплекс технічного захисту інформації”* (відповідно до “Положення про технічний захист інформації в Україні”, введеного в дію указом Президента України від 27 вересня 1999 року № 1229/99).

22. Хто належить до суб'єктів системи ТЗІ держави (відповідно до “Положення про технічний захист інформації в Україні”, введеного в дію указом Президента України від 27 вересня 1999 року № 1229/99)?

23. Відповідно до положень НД ТЗІ 1.4-001-2000 надати відповіді на питання:

яка мета створення Служби захисту інформації (далі – СЗІ) в установі?

яким організаційно-розпорядчим документом установи визначаються завдання, функції (повноваження) та відповідальність посадових осіб служби захисту інформації установи?

яке відношення мають посадові особи СЗІ до організації навчання персоналу підрозділів установи з питань забезпечення захисту інформації під час роботи на АРМ ІКС?

24. Доповісти про етапи створення КСЗІ в ІКС, які визначені нормативними документами, чинними у сфері ТЗІ (назвати ці НД ТЗІ).

25. Надати визначення (або пояснення) таким термінам:

“політика безпеки інформації в АС”;

“план захисту інформації в АС”;

“аудит інформаційної безпеки”.

26. Доповісти про призначення та спрямованість змісту таких нормативних документів:

НД ТЗІ 3.6-008-21 “Порядок моніторингу безпеки інформаційних систем”;

“Порядок здійснення державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури” (затверджений наказом Адміністрації Держспецзв’язку від 08 квітня 2021 року № 61/ДСК).

27. Доповісти про види інспекційних перевірок стану ТЗІ в установах держави, які здійснюються Держспецзв'язком України в ході проведення контрольно-інспекторської роботи з питань ТЗІ.

28. Доповісти про призначення та спрямованість змісту наступних нормативних документів:

“Положення про державну експертизу в сфері технічного захисту інформації” (наказ Адміністрації Держспецзв’язку від 16.05.2007 № 93, зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087).

НД ТЗІ 2.6-001-11 “Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах”.

29. Відповідно до “Положення про державну експертизу в сфері технічного захисту інформації” (наказ Адміністрації Держспецзв’язку від 16.05.2007 № 93, зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087) доповісти про:

мету державної експертизи в сфері ТЗІ та у який спосіб вона може проводитись;

перелік суб’єктів державної експертизи в сфері ТЗІ;

перелік об’єктів державної експертизи в сфері ТЗІ.

послідовність проведення державної експертизи в сфері ТЗІ.

Розділ 3
ОСНОВИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

3.1 Загальні положення нормативно-правового забезпечення криптографічного захисту інформації в Україні

Сектор інформаційної безпеки, пов'язаний з криптографічним захистом інформації, як усі інші сектори, які були раніше розглянуті в цьому посібнику, охоплює десятки нормативно-правових та нормативних документів, вимогами яких регламентуються усі складові організації та здійснення криптографічного захисту інформації, а також забезпечення гарантій захисту інформації в результаті її криптографічного захисту.

У межах освітнього компонента "Нормативно-правове забезпечення інформаційної безпеки" здобувачам вищої освіти доцільно вивчити базові НПА, які складають основу нормативно-правового забезпечення криптографічного захисту інформації в Україні. До таких НПА належать:

"Положення про порядок здійснення криптографічного захисту інформації в Україні" (указ Президента України від 22 травня 1998 року № 505/98);

"Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації" (затверджено наказом Адміністрації Держспецзв'язку від 20 липня 2007 року за № 141);

постанова КМУ від 16 листопада 2016 року № 821 "Про деякі питання ліцензування господарської діяльності в галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України".

3.1.1 "Положення про порядок здійснення криптографічного захисту інформації в Україні" (указ Президента України від 22 травня 1998 року № 505/98). Категорії інформації, що потребують криптографічного захисту в разі її передачі технічними засобами

Першим у переліку наведено ***"Положення про порядок здійснення криптографічного захисту інформації в Україні" (указ Президента України від 22 травня 1998 року № 505/98)*** *(далі – Положення)***.** В історичному контексті в 90-ті роки після здобуття Україною незалежності, взяття курсу на стрімкий розвиток та інтенсивне впровадження в усі сфери функціонування держави передових цифрових технологій розпочався активний процес трансформації застарілої пострадянської нормативно-

правової бази в сучасне нормативно-правове забезпечення усіх секторів інформаційної безпеки держави, зокрема й у сфері криптографічного захисту інформації.

Одним із перших головних НПА в цій сфері, в якому були визначені головні нормативно-правові аспекти функціонування системи криптографічного захисту інформації в державі, стало це *Положення.*

В НПА на юридичному рівні було встановлено: [50]

статус Державної служби спеціального зв'язку та захисту інформації України *(далі – Держспецзв'язку України)* як головного провідника державної політики у сфері криптографічного захисту інформації, а також державного органу, з яким погоджуються усі питання проєктування, виробництва, закупівель, продажу, застосування, утилізації засобів криптографічного захисту інформації;

обов’язковість ліцензування будь-якої діяльності в державі, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації;

обов’язковість проведення сертифікаційних випробувань криптосистем і засобів криптографічного захисту, які створюються для захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави. Зазначені криптосистеми і засоби *можуть перебувати тільки в державній власності.* Криптосистеми й засоби криптографічного захисту, які використовуються для захисту конфіденційної інформації обов’язково повинні мати *сертифікат відповідності* встановленого зразку;

обов’язковість регламентації будь-якого виду діяльності у сфері криптографічного захисту інформації вимогами відповідних *інструкцій, положень, правил, настанов*, погоджених із Держспецзв'язку України;

обов’язковість наявності допуску до державної таємниці в осіб, діяльність яких буде пов’язана з користуванням криптосистемами або засобами криптографічного захисту секретної інформації, яка є власністю держави.

відповідальність згідно із законодавством України осіб у разі порушення вимог НПА у сфері криптографічного захисту інформації.

Положеннями цього НПА встановлено, що обов’язкового криптографічного захисту в разі її передачі технічними засобами потребує інформація наступних категорій:

– інформація, яка становить державну або іншу передбачену законом таємницю (далі – таємна інформація);

– службова інформація, яка є власністю держави;

– конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації";

Отже, короткий за обсягом, але дуже інформативний за змістом цей НПА чітко накреслює напрямки нормативно-правового забезпечення в даному секторі ІБ. Із його положень стає зрозумілим, що кожний напрямок діяльності в сфері криптографічного захисту інформації, а саме: розробка, виготовлення, ввезення, вивезення, реалізація, використання, утилізація засобів криптографічного захисту інформації, надання будь-яких послуг із криптографічного захисту інформації тощо, повинні бути чітко регламентовані вимогами відповідних правил, інструкцій, положень, настанов. Ці нормативні документи повинні пройти обов'язкову процедуру погодження з Держспецзв'язком України.

Положення таких основних нормативних документів, що знаходяться у відкритому доступі, розглядаються нижче. Ця робота щодо вивчення НПА та нормативних документів, доступ до змісту яких обмежений, буде тривати в подальшому під час навчальних занять зі спеціальних дисциплін, таких як "Засоби та комплекси криптографічного захисту інформації – 1", "Засоби та комплекси криптографічного захисту інформації – 2","Безпека спеціального зв'язку".

3.1.2 "Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації" (затверджено наказом Адміністрації Держспецзв'язку від 20 липня 2007 року за № 141)

Другим важливим НПА є ***"Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації" (затверджено наказом Адміністрації Держспецзв'язку від 20 липня 2007 року за № 141))***, вимогами якого регламентуються процедури розроблення, виготовлення, експлуатації та утилізації засобів криптографічного захисту інформації різних видів та призначення.

З огляду на те, що в нашій державі десятки установ, підприємств, організацій мають ліцензію (спеціальний дозвіл) на розробку, виготовлення, продаж різних за призначенням засобів криптозахисту, а сотні – залучені до їх експлуатації, стають зрозумілими актуальність та необхідність наявності в державі цього нормативно-правового документа.

Документ *має за мету встановлення в державі єдиного порядку розроблення, виробництва та експлуатації засобів криптографічного захисту інформації та засобів електронного цифрового підпису.*

Вимоги цього *Положення* обов'язкові для виконання державними органами, підприємствами, установами і організаціями незалежно від форм власності (далі – організації), діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) та експлуатацією засобів КЗІ. Винятком є Національний банк України, який може розробляти засоби КЗІ, призначені виключно для забезпечення власних потреб та потреб банківської системи України, без погодження з Адміністрацією Держспецзв'язку. В цьому випадку Нацбанк України у своїх нормативних документах з цих питань повинен враховувати вимоги даного *Положення*.

Загальний зміст даного *Положення* міститься на 17 аркушах (шрифт 12) та складається із 5 розділів: [51]

розділ I – Загальні положення;

розділ II – Розроблення засобів КЗІ;

розділ III – Виробництво засобів КЗІ;

розділ IV – Експлуатація засобів КЗІ;

розділ V– Виведення з експлуатації та утилізація (знищення) засобів КЗІ.

розділ I – Загальні положення

В *розділі I – Загальні положення* наведені тлумачення основних термінів у сфері криптографічного захисту інформації для правильного розуміння усіма суб'єктами положень цього та інших НПА у сфері КЗІ, а також надані роз'яснення щодо можливих типів засобів КЗІ, їхніх особливостей побудови та функціонування для правильного розуміння подальших вимог документа та їхнього практичного виконання.

Так, залежно *від способу реалізації* розрізняють такі *три типи засобів КЗІ*:

апаратні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовано в оптичних, механічних, електронних або інших спеціалізованих пристроях та не може бути змінено без зміни цих пристроїв;

апаратно-програмні засоби, алгоритм функціонування (або окремі функції, у тому числі криптографічні) яких реалізовано в їхніх спеціально для цього використаних апаратних компонентах (програмованих логічних інтегральних схемах, контролерах) і заміна алгоритму функціонування (або окремих функцій, у тому числі криптографічних) яких можлива виробником цих засобів без зміни апаратних компонентів;

програмні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовано програмним забезпеченням, що працює під управлінням операційної системи обчислювальних або комунікаційних пристроїв загального призначення і може бути змінено

розробником цього програмного забезпечення, при цьому для роботи засобу непотрібні додаткові спеціально застосовані апаратні компоненти.

Залежно *від виконання* встановлюються такі види засобів КЗІ:

вид А – засоби, які на конструктивному, алгоритмічному та програмному рівнях *є єдиними виробами*, *що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів*.

вид Б – засоби, які на конструктивному, алгоритмічному та програмному рівнях *є єдиними виробами та призначені для використання у складі комплексів оброблення та передавання інформації*.

Засоби виду Б поділяються на:

підвид Б1 – вироби, які встановлюються в розрив каналу електронних комунікацій та/або розділяють потоки захищеної інформації та інформації, що підлягає захисту, а також вироби, що забезпечують відокремлення оброблення захищеної інформації та інформації, що підлягає захисту, в обчислювальній системі;

підвид Б2 – апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням.

вид В – криптографічні модулі, які не використовуються (не експлуатуються) окремо, а застосовуються як складові частини при побудові засобів КЗІ видів А та Б.

Залежно *від призначення* встановлюються такі *категорії засобів КЗІ:*

засоби шифрування інформації (далі – засоби *категорії «Ш»*);

засоби, призначені *для виготовлення ключових даних або ключових документів* (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ (далі – засоби *категорії «К»*);

засоби, що *реалізують криптоперетворення та/або механізми імітозахисту* та призначені для забезпечення захисту (підтвердження) хоча б однієї з таких властивостей інформації: справжності (авторства), цілісності, неспростовності, дати створення (далі – засоби *категорії «П»*);

засоби *захисту інформації від несанкціонованого доступу* (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (далі – засоби *категорії «Р»*);

засоби (або засоби, об’єднані в комплекси), спеціально призначені для *розроблення, дослідження, виробництва та випробувань засобів КЗІ*, у тому числі програмування та/або запису в їхні апаратні компоненти (програмовані логічні інтегральні схеми, контролери), перевірки та контролю правильності реалізації в засобах КЗІ криптографічних функцій (далі – засоби *категорії «З»*).

В загальних положеннях визначений перелік суб’єктів, які в процесі розроблення, виробництва та експлуатації засобів КЗІ беруть участь і взаємодіють між собою, та їхні повноваження:

Адміністрація Держспецзв'язку;

замовники;

розробники;

виробники;

організації, що експлуатують засоби КЗІ;

організації, що проводять сертифікаційні випробування (експертні роботи);

постачальники ключових документів.

В цьому розділі зроблено наголос *на обов’язковості ліцензування діяльності суб’єктів* на право провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг).

Встановлений порядок можливого поширення інформації з питань КЗІ, яка надається Адміністрацією Держспецзв'язку, суб'єктами господарювання – тільки за погодженням з Адміністрацією Держспецзв'язку.

Адміністрація Держспецзв'язку забезпечує конфіденційність інформації та дотримання авторських прав щодо наданих їй матеріалів.

розділ ІІ – Розроблення засобів КЗІ

Розроблення засобів КЗІ здійснюється шляхом виконання відповідних науково-дослідних робіт (далі – НДР) з розроблення нових принципів побудови і функціонування засобів КЗІ та дослідно-конструкторських робіт (далі – ДКР) зі створення нових або модернізації наявних зразків засобів КЗІ.

НДР (або ДКР) виконуються згідно з технічними завданнями (далі – ТЗ), які погоджуються Виконавцем НДР (ДКР).

Погоджене Виконавцем ТЗ на НДР (ДКР) надсилається до Адміністрації Держспецзв'язку, яка протягом одного місяця його погоджує або надає умотивовану відмову.

За результатами НДР готується ТЗ на ДКР з розроблення нового або модернізації наявного зразка засобу КЗІ з підготовкою (за необхідності) техніко-економічного обґрунтування ДКР. В змісті ТЗ особлива увага приділяється забезпеченню безпеки системи управління ключовими даними (ключами). Залежно від ймовірних умов експлуатації засобів КЗІ та відповідно до цінності інформації, що захищається, обґрунтовується вибір відповідного класу засобів КЗІ (п.п. 8, 9 класи А1, Б1, Б2, В1, В2, В3). Класи засобів КЗІ наведено в порядку зменшення вимог таким чином, що

рівень, наведений вище, передбачає виконання вимог усіх наведених нижче класів.

Встановлено обов'язкове інформативне наповнення змісту ТЗ на ДКР (п.10). Зроблено акцент на використанні у засобах КЗІ криптоалгоритмів та криптопротоколів, які є національними стандартами, або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв'язку видано позитивний експертний висновок. Інші криптоалгоритми та криптопротоколи для використання виключно в банківській системі України погоджуються Адміністрацією Держспецзв'язку за відповідним зверненням та обґрунтуванням Національного банку України.

Методики генерації ключових даних та управління ключами погоджуються з Адміністрацією Держспецзв'язку. Можливість погодження цих методик визначається за результатами державної експертизи у сфері криптографічного захисту інформації.

Засоби КЗІ розробляються з урахуванням можливих загроз у ймовірних умовах їх експлуатації.

У засобах КЗІ повинні бути реалізовані методи захисту, що відповідають установленим вимогам, залежно від виду, типу, категорії та класу засобу КЗІ (в п. 14 встановлені обов'язкові механізми захисту для різних класів КЗІ).

В п. 17 визначені обов'язки Розробника ЗКЗІ щодо розробки робочої конструкторської документації, її складу та обов'язкової наявності в ній проєкту технічних умов, експлуатаційних документів, інструкції із забезпечення безпеки експлуатації засобу КЗІ, інструкції щодо порядку генерації ключових даних і поводження (облік, зберігання, знищення) з ключовими документами (обов'язково для засобів КЗІ видів А та Б, підвидів Б1 та Б2), а також інструкції про порядок застосування виробу в складі засобу КЗІ виду А або Б, підвидів Б1 та Б2 (для засобів КЗІ виду В). Проєкт технічних умов погоджується з Адміністрацією Держспецзв'язку.

В п. п. 19, 20 визначено обов'язкове інформативне наповнення документів, що входять до складу робочої конструкторської документації на ЗКЗІ.

Під час виконання ДКР Розробник передбачає створення устаткування (допоміжного обладнання) для проведення сертифікаційних випробувань (експертних робіт) засобу КЗІ.

Із виготовленням дослідних зразків ЗКЗІ Замовником та Розробником на ділянці останнього проводяться їх випробування. На випробуваннях окрім заявлених технічних та експлуатаційних характеристик перевіряються й ефективність та достатність організаційно-технічних заходів щодо забезпечення безпеки інформації. За результатами випробувань складається Звіт, який затверджується Замовником.

Звіт надсилаються до Адміністрації Держспецзв'язку під час проведення державної експертизи ЗКЗІ у сфері КЗІ.

Позитивний експертний висновок за результатами державної експертизи у сфері КЗІ щодо засобу КЗІ є погодженням Адміністрації Держспецзв'язку інструкції із забезпечення безпеки експлуатації засобу КЗІ та інструкції щодо порядку поводження з ключовими документами.

Порядок забезпечення режиму безпеки під час розроблення засобів КЗІ визначається Розробником в окремій інструкції, в якій наводяться вимоги щодо поводження із засобами КЗІ, обладнання приміщень, заходи із запобігання компрометації засобів КЗІ тощо.

розділ ІІІ – Виробництво засобів КЗІ

Виробництво засобів КЗІ здійснюється тільки за наявності чинного сертифіката відповідності (позитивного експертного висновку) на засіб КЗІ та на засоби (комплекси), призначені для розроблення, дослідження, виробництва та випробувань засобів КЗІ (у разі його використання), ТУ та інструкції із забезпечення безпеки експлуатації засобів КЗІ.

В п. 2 даного розділу визначені обов'язки Виробника ЗКЗІ.

Виробництво засобів КЗІ здійснюється з використанням тільки ліцензійного програмного забезпечення або за погодженням із Замовником комп'ютерних програм вільного використання, які повинні бути забезпечені документацією, що підтверджує правомірність їх використання згідно з ліцензією або належність до комп'ютерних програм вільного використання.

розділ IV – Експлуатація засобів КЗІ

Для криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, використовуються засоби КЗІ, які мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ, що підтверджують клас засобу КЗІ (рівень гарантій) та реалізовані методи захисту, а суб'єкти, що їх використовують, мають на це права.

Державна експертиза у сфері криптографічного захисту інформації проводиться в порядку, визначеному відповідними нормативно-правовими актами. (п. 1).

Підставою для початку експлуатації таких засобів КЗІ в організації, є відповідний акт організаційно-розпорядчого характеру цієї організації (п. 2).

Кожний екземпляр засобів КЗІ береться на облік в організації з дати їх отримання (п. 3).

Облік здійснюється у відповідному журналі обліку засобів КЗІ та носіїв ключової інформації до них. Облік програмних засобів КЗІ

здійснюється за формулярами на кожну ПЕОМ, на якій встановлено (проінстальовано) такий засіб. Журнал обліку повинен містити встановлені облікові відомості, за якими ЗКЗІ ідентифікується та закріплюється (п. 3).

Одиницею обліку кожного екземпляра засобу КЗІ є:

для апаратних та апаратно-програмних засобів – конструктивно закінчений технічний засіб;

для програмних засобів – інсталяційна дискета, компакт-диск (CD, DVD) тощо;

ПЕОМ користувачів, на яких встановлено (проінстальовано) програмні засоби КЗІ.

Облік засобів КЗІ та носіїв ключової інформації до них в організації забезпечується відповідальними особами, визначеними відповідними актами організаційно-розпорядчого характеру цієї організації.

Збереження засобів КЗІ, носіїв ключової інформації забезпечується відповідальною особою, функціональними обов'язками якої це визначено (п. 3).

Передача засобів КЗІ здійснюється на підставі відповідних договорів, у яких вказується порядок встановлення засобів КЗІ у користувачів та обслуговування цих засобів, забезпечення ключовими документами (ключовими даними), а також ужиття заходів щодо забезпечення режиму безпеки тощо (п. 4).

Експлуатація засобів КЗІ в установах здійснюється у повній відповідності до вимог експлуатаційної документації, інструкції із забезпечення безпеки експлуатації засобів КЗІ, а також інструкції щодо порядку генерації ключових даних та поводження з ключовими документами (п. 6).

Постачання ключових документів (ключових даних) до засобів КЗІ постачальником ключових документів організаціям, які експлуатують засоби КЗІ, здійснюється у порядку, встановленому Адміністрацією Держспецзв'язку.

Ключові документи, отримані від постачальника ключових документів, не можуть тиражуватися або використовуватися для інших засобів КЗІ, якщо це не передбачено договором про постачання ключових документів (п. п. 7, 8).

Засоби КЗІ без уведених ключових даних мають гриф обмеження доступу, який відповідає грифу обмеження доступу до опису криптосхеми. Гриф обмеження доступу засобів КЗІ з уведеними ключовими даними визначається грифом обмеження доступу до ключових документів, але не нижче грифа обмеження доступу до опису криптосхеми (п. 10).

Гриф обмеження доступу до ключових документів, що використовуються для криптографічного захисту інформації, повинен відповідати грифу обмеження доступу до інформації, що захищається (п. 11).

Застосування засобів КЗІ під час міжнародного обміну інформацією здійснюється відповідно до законодавства та міжнародних угод (договорів) України (п. 12).

<u>розділ V – Виведення з експлуатації та утилізація (знищення) засобів КЗІ.</u>

Засоби КЗІ, які стали непридатними до використання або характеристики яких не відповідають сучасним вимогам щодо криптографічного захисту інформації, виводяться з експлуатації відповідно до вимог інструкції із забезпечення безпеки експлуатації засобів КЗІ (п. 1).

Утилізація (знищення) засобів КЗІ проводиться відповідно до вимог інструкції із забезпечення безпеки експлуатації засобів КЗІ (п. 2).

Порядок утилізації (знищення) засобів КЗІ, вироблених для потреб Національного банку України і потреб банківської системи України, визначається Національним банком України (п. 3).

Отже, *"Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації" (затверджено наказом Адміністрації Держспецзв'язку від 20 липня 2007 року за № 141) встановлює загальний порядок виконання обов'язкових заходів на етапах розроблення, виробництва, експлуатації, утилізації засобів КЗІ. Різноманіття видів засобів криптографічного захисту інформації, особливості їх призначення та побудови повинні враховуватися під час усіх етапів їхнього життєвого циклу.*

На підставі цього висновку можна зробити припущення, що окрім загальних вимог, визначених даним НПА, стосовно кожного із видів ЗКЗІ повинні бути розроблені додаткові нормативні документи, якими будуть регламентовані вимоги щодо розроблення, сертифікації, виготовлення, застосування, утилізації конкретних ЗКЗІ *з урахуванням їхніх особливостей.*

На практиці такі припущення стають цілком реальними речами, і в подальшому навчальному процесі здобувачі вищої освіти переконаються у правильності такого ствердження, коли будуть вивчати цілу низку нормативних документів, що встановлюють правила експлуатації та

поводження із ЗКЗІ різних видів на заняттях зі спеціальних навчальних дисциплін, що були вказані вище.

3.1.3 “Про деякі питання ліцензування господарської діяльності у галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України” (постанова КМУ від 16 листопада 2016 року № 821)

З положень вище розглянутих НПА відомо, що загальною вимогою для провадження діяльності у галузі криптографічного захисту інформації різними суб’єктами є *наявність у них ліцензії*. Тому є логічним докладніше розглянути положення чинних в державі НПА, які регламентують ці питання.

Чинним законодавством держави, а саме *Законом України “Про ліцензування видів господарської діяльності” від 2 березня 2015 року № 222-VIII* встановлено юридичні підстави ліцензування діяльності суб’єктів у галузі криптографічного захисту інформації поряд з іншими видами господарської діяльності. Саме в положеннях *п. 8 статті 7 Перелік видів господарської діяльності, що підлягають ліцензуванню* цього закону вказано: [52]

Стаття 7. Ліцензуванню підлягають такі види господарської діяльності:

1) банківська діяльність, діяльність з надання фінансових послуг та діяльність з надання банкам послуг з інкасації;

. . . . . .

8) надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України;

. . . . . .

Наступним головним НПА з питань ліцензування господарської діяльності у галузі криптографічного захисту інформації є *постанова КМУ від 16 листопада 2016 року № 821 “Про деякі питання ліцензування господарської діяльності у галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України”*.

Саме цією постановою КМУ ухвалені: [53]

“Перелік послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню” *(далі – Перелік послуг)**;***

“***Ліцензійні умови провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України”*** *(далі – Ліцензійні умови).*

Перелік послуг встановлює види діяльності суб’єктів у галузі КЗІ та ТЗІ, які вимагають оформлення ліцензії, та відповідно складається із двох розділів:

I. Послуги у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), господарська діяльність щодо яких підлягає ліцензуванню

1. Розроблення і складення конструкторської та іншої технічної документації, виробництво криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

2. Постачання, монтаж (встановлення), налаштування, технічне обслуговування (супроводження), ремонт та/або утилізація криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

3. Тематичні та експертні дослідження криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

II. Послуги у галузі технічного захисту інформації, Господарська діяльність щодо яких підлягає ліцензуванню

1. Оцінювання захищеності інформації, що не становить державної таємниці.

2. Оцінювання захищеності інформації усіх видів, зокрема інформації, що становить державну таємницю.

3. Виявлення закладних пристроїв.

Ліцензійні умови встановлюють термінологію видів господарської діяльності в галузі КЗІ та ТЗІ, загальний порядок отримання ліцензії в цій галузі; надають вичерпний перелік документів, що додаються до заяви про одержання ліцензії; визначають кадрові, організаційні та технологічні вимоги, обов'язкові для виконання під час провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису).

Структура даного НПА:

текстова частина:

Загальні положення (п. п. 1 – 9).

Вимоги щодо провадження ліцензованої діяльності у галузі криптографічного захисту інформації

кадрові вимоги (п. п. 10 – 16);

організаційні вимоги (п. п. 17 – 21);

технологічні вимоги (п. п. 22 – 28).

Вимоги щодо провадження ліцензованої діяльності у галузі технічного захисту інформації

кадрові вимоги (п. п. 29 – 33);

організаційні вимоги (п. п. 34 – 39);

технологічні вимоги (п. п. 40 – 44).

додатки (додатки 1 – 16 до Ліцензійних умов):

Додаток 1 – Заява про одержання ліцензії;

Додаток 2 – Відомості про наявність спеціалістів, необхідних для надання відповідних видів послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації;

Додаток 3 – Відомості про наявність засобів вимірювальної техніки та контролю, допоміжних засобів та обладнання, інформаційних (автоматизованих) систем та/або технічних засобів обробки інформації, що забезпечують надання відповідних видів послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації;

Додаток 4 – Відомості про наявність нормативно-правової бази, що забезпечує надання відповідних видів послуг у галузі криптографічного

захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації;

Додаток 5 – Відомості про наявність спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею;

Додаток 6 – Відомості про наявність відповідних приміщень, засобів обчислювальної техніки, інформаційних і телекомунікаційних систем (комплексів), необхідних для надання відповідних видів послуг у галузі криптографічного захисту інформації;

Додаток 7 – Відомості про наявність власних або орендованих службових, виробничих приміщень, необхідних для надання відповідних видів послуг у галузі криптографічного захисту інформації;

Додаток 8 – Відомості про наявність інформаційних (автоматизованих) систем та/або технічних засобів обробки секретної інформації, необхідних для надання відповідних видів послуг у галузі технічного захисту інформації;

Додаток 9 – Відомості про наявність об’єктів інформаційної діяльності для проведення секретних нарад, обговорень і робіт з технічного захисту інформації;

Додаток 10 – Опис документів, що додаються до заяви про отримання ліцензії;

Додаток 11 – Заява про переоформлення ліцензії;

Додаток 12 – Заява про звуження провадження господарської діяльності

Додаток 13 – Заява про розширення провадження господарської діяльності;

Додаток 14 – Відомості про надані послуги з криптографічного захисту інформації;

Додаток 15 – Відомості про надані послуги з технічного захисту інформації;

Додаток 16 – Рекомендований перелік засобів вимірювальної техніки та контролю і обладнання, необхідних для надання послуг у галузі технічного захисту інформації, що підлягають ліцензуванню.

Загальний порядок отримання суб’єктами ліцензії у галузі КЗІ полягає у наступному:

1. Ліцензуванню підлягає господарська діяльність суб’єктів із надання послуг у галузі криптографічного захисту інформації, зазначених у розділі І *Переліку послуг*;

2. Суб’єкт діяльності з надання послуг у сфері КЗІ (здобувач ліцензії) подає у встановленому законом порядком до органу ліцензування *Заяву про одержання ліцензії* (додаток 1) разом з документами, визначеними у Законі.

До заяви про одержання ліцензії на провадження ліцензованої діяльності за підписом здобувача ліцензії додаються підтвердні документи (додатки 2 – 9).

Заява про одержання ліцензії та документи, що додаються до неї, приймаються згідно з описом (додаток 10).

Документи, копії яких подаються до органу ліцензування відповідно до Закону, та документи (копії), що підтверджують достовірність даних, зберігаються ліцензіатом протягом дії ліцензії.

3. Орган ліцензування протягом п’яти робочих днів з дня одержання заяви про отримання ліцензії встановлює наявність або відсутність підстав для залишення її без розгляду і в разі їх наявності ухвалює відповідне рішення.

4. У разі встановлення під час розгляду заяви про отримання ліцензії відсутності підстав для відмови у видачі ліцензії орган ліцензування ухвалює рішення про видачу ліцензії.

Строк ухвалення рішення про видачу ліцензії або про відмову в її видачі становить *десять робочих днів* з дня одержання органом ліцензування заяви про отримання ліцензії.

Рішення набирає чинності та оприлюднюється на офіційному веб-сайті органу ліцензування, а інформація про таке рішення вноситься до ліцензійного реєстру наступного робочого дня після його прийняття. У рішенні про видачу ліцензії орган ліцензування зазначає реквізити рахунку для внесення плати за видачу ліцензії.

5. Ліцензія на провадження здобувачем ліцензії визначеного ним виду господарської діяльності, оформлюється органом ліцензування в *електронному вигляді* (запис про рішення органу ліцензування щодо видачі ліцензії суб’єкту господарювання в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань) та відображається у виписці з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, яка видається ліцензіату безоплатно, та підлягає обов’язковому оприлюдненню на порталі електронних сервісів у порядку, визначеному Міністерством юстиції України в Порядку надання відомостей з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань.

Ліцензія видається на необмежений строк.

У встановленому законодавчими та нормативно-правовими актами порядку ліцензування діяльності із надання послуг в сфері КЗІ дуже важливе значення має точність та достовірність надання здобувачем ліцензії необхідних відомостей (додатки 2 – 9) щодо виконання ліцензійних умов. У зв'язку із цим є нагода ліцензійні умови господарської

діяльності в галузі криптографічного захисту інформації розглянути докладно.

3.1.4 Ліцензійні умови господарської діяльності в галузі криптографічного захисту інформації

Вимоги щодо провадження ліцензованої діяльності у галузі криптографічного захисту інформації:

Кадрові вимоги:

10. Здобувач ліцензії чи ліцензіат у галузі криптографічного захисту інформації повинен мати:

затверджену керівником суб'єкта господарювання організаційну структуру, в якій зазначені підрозділи або спеціалісти, які забезпечать виконання адміністративно-керівних, виробничо-технічних функцій щодо заявленого виду послуг;

положення про структурні підрозділи або посадові інструкції працівників, що залучаються до безпосереднього провадження заявленого виду діяльності, затверджені в установленому порядку та складені з урахуванням штатного розпису, розподілу обов'язків, повноважень працівників;

інженерно-технічних працівників і робітників, склад, професія та кваліфікація яких відповідає організаційній структурі суб'єкта господарювання.

11. Виконавці робіт залежно від заявленого виду послуг повинні мати відповідний освітній та освітньо-кваліфікаційний рівень.

Керівники виробничих та функціональних підрозділів повинні мати вищу освіту відповідного рівня та ступеня (магістр, спеціаліст) у галузі знань "Інформаційна безпека" або вищу інженерно-технічну освіту фахового спрямування відповідно до обраного виду послуг з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань криптографічного захисту інформації за напрямами підготовки відповідно до обраного виду послуг або стаж роботи у галузі криптографічного захисту інформації за обраним видом послуг не менш як три роки.

Професіонали та фахівці повинні мати вищу освіту відповідного рівня та ступеня (магістр, спеціаліст, бакалавр, молодший спеціаліст).

12. До виконавців робіт з надання послуг з розроблення і складення конструкторської та іншої технічної документації, виробництва криптосистем і засобів криптографічного захисту інформації (з наданням права на провадження діяльності у галузі криптографічного захисту

інформації, що становить державну таємницю; права на провадження діяльності у галузі криптографічного захисту службової інформації) встановлюються такі кадрові вимоги:

до головного конструктора або фахівця, на якого покладено обов'язки головного конструктора, – вища освіта відповідного рівня та ступеня (магістр, спеціаліст), стаж роботи на посаді керівника нижчого рівня не менш як три роки, спеціалізація за освітою відповідно до розділів (частин) технічного завдання та/або проєкту, а також досвід із створення продукції оборонного призначення (у разі виконання функцій генерального проєктувальника криптосистем і засобів криптографічного захисту інформації за державним оборонним замовленням);

до виконавця робіт – вища освіта відповідного рівня та ступеня (магістр, спеціаліст, бакалавр, молодший спеціаліст), стаж роботи за професією не менш як три роки, спеціалізація за освітою відповідно до розділів (частин) технічного завдання та/або проєкту;

до інших професіоналів, фахівців – відповідно до організаційної структури суб'єкта господарювання, спеціалізація за освітою відповідно до розділів (частин) технічного завдання та/або проєкту.

13. До виконавців робіт з надання послуг з постачання, монтажу (встановлення), налаштування, технічного обслуговування (супроводження), ремонту та/або утилізації криптосистем і засобів криптографічного захисту інформації (з наданням права на провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; права на провадження діяльності у галузі криптографічного захисту службової інформації) встановлюються такі кадрові вимоги:

до головного інженера або фахівця, на якого покладено обов'язки головного інженера, – вища освіта відповідного рівня та ступеня (магістр, спеціаліст), стаж роботи на посаді керівника нижчого рівня не менш як три роки, спеціалізація за освітою відповідно до видів послуг з постачання, монтажу, налаштування, технічного обслуговування (супроводження), ремонту та/або утилізації криптосистем і засобів криптографічного захисту інформації;

до виконавця робіт – вища освіта відповідного рівня та ступеня (магістр, спеціаліст, бакалавр, молодший спеціаліст), стаж роботи за професією не менш як три роки, спеціалізація за освітою відповідно до видів послуг з постачання, монтажу, налаштування та технічного обслуговування (супроводження), ремонту та/або утилізації криптосистем і засобів криптографічного захисту інформації;

до інших професіоналів, фахівців – відповідно до організаційної структури суб'єкта господарювання, спеціалізація за освітою відповідно до видів послуг з постачання, монтажу, налаштування та технічного обслуговування (супроводження), ремонту та/або утилізації криптосистем і

засобів криптографічного захисту інформації.

14. До виконавців робіт з надання послуг з тематичних та експертних досліджень криптосистем і засобів криптографічного захисту інформації (з наданням права на провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; права на провадження діяльності у галузі криптографічного захисту службової інформації) встановлюються такі кадрові вимоги:

до виконавця робіт – вища освіта відповідного рівня та ступеня (магістр, спеціаліст, бакалавр, молодший спеціаліст), стаж роботи за професією не менш як три роки, спеціалізація за освітою відповідно до видів послуг з проведення тематичних та експертних досліджень криптосистем і засобів криптографічного захисту інформації;

до інших професіоналів, фахівців – відповідно до організаційної структури суб'єкта господарювання, спеціалізація за освітою відповідно до видів послуг з проведення тематичних та експертних досліджень криптосистем і засобів криптографічного захисту інформації.

До стажу роботи у галузі криптографічного захисту інформації зараховується стаж роботи та/або служби на посадах у суб'єктів системи криптографічного захисту інформації, посадові обов'язки за якими передбачають виконання завдань з криптографічного захисту інформації, пов'язаних з обраними видами послуг.

15. Спеціалісти відповідно до своїх функціональних обов'язків повинні вміти:

користуватися наявним обладнанням, що забезпечує надання обраного виду послуг;

здійснювати обробку результатів наданих згідно з ліцензією послуг та оформляти звітні (підсумкові) документи.

16. Керівник суб'єкта господарювання та керівники виробничих і функціональних підрозділів повинні працювати у суб'єкта господарювання за основним місцем роботи відповідно до штатного розпису.

Організаційні вимоги

17. Ліцензіат у галузі криптографічного захисту інформації повинен зберігати:

документи, копії яких подавалися органу ліцензування відповідно до вимог Закону, та документи (копії), які підтверджують достовірність даних, що зазначалися здобувачем ліцензії у документах, які подавалися органу ліцензування відповідно до вимог Закону та цих Ліцензійних умов (протягом дії ліцензії);

документи, що підтверджують внесення плати за видачу ліцензії (протягом дії ліцензії);

примірники звітних (підсумкових) документів, розроблених під час

надання згідно з ліцензією послуг (на паперових носіях або у вигляді електронних документів протягом строку, визначеного у договорі між ним і замовником послуг, але не менш як п’ять років);

договори оренди обладнання, що забезпечує надання відповідних видів послуг у галузі криптографічного захисту інформації (протягом п’яти років);

документи (копії), що засвідчують повірку власних та орендованих (у разі оренди обладнання) засобів вимірювальної техніки (протягом п’яти років).

18. Ліцензіат зобов’язаний повідомляти органу ліцензування про зміну даних (зокрема розширення, звуження провадження виду господарської діяльності), які зазначені в його документах, що додавалися до заяви про одержання ліцензії, у строк не пізніше ніж один місяць з дня настання таких змін.

19. На письмове звернення органу ліцензування ліцензіат інформує про результати ліцензованої діяльності у галузі криптографічного захисту інформації (додаток 14).

20. Під час проведення органом ліцензування в установленому законодавством порядку перевірки додержання ліцензіатом у галузі криптографічного захисту інформації вимог цих Ліцензійних умов повинен бути присутнім керівник ліцензіата чи його заступник або інша уповноважена особа ліцензіата.

21. У разі планового або позапланового припинення ліцензованої діяльності у галузі криптографічного захисту інформації (у зв’язку з неможливістю використання (відсутністю) матеріально-технічної бази (засобів вимірювальної техніки та контролю і обладнання, допоміжних засобів, інформаційних (автоматизованих) систем та/або технічних засобів обробки інформації), необхідної для надання відповідних видів послуг у галузі криптографічного захисту інформації, виникненням обставин непереборної сили тощо) ліцензіат для відновлення такої діяльності зобов’язаний забезпечити виконання вимог цих Ліцензійних умов.

Технологічні вимоги

22. Здобувач ліцензії чи ліцензіат у галузі криптографічного захисту інформації повинен мати:

службові та виробничі приміщення, які забезпечують технологічні умови надання відповідних видів послуг у галузі криптографічного захисту інформації;

власні або на праві користування засоби вимірювальної техніки та контролю і обладнання, допоміжні засоби, інформаційні (автоматизовані) системи та/або технічні засоби обробки інформації, що забезпечують надання відповідного виду послуг у галузі криптографічного захисту

інформації відповідно до встановлених технологічних вимог, пройшли відповідно до вимог нормативної документації технічне обслуговування та перебувають у належному технічному стані;

нормативно-правову базу (нормативно-правові акти та стандарти у сфері криптографічного захисту інформації, інші стандарти та нормативні документи в електронному вигляді або на паперових носіях (акти та документи, що мають гриф обмеження доступу, лише на паперових носіях), що забезпечує надання відповідного виду послуг у галузі криптографічного захисту інформації. Перелік таких документів визначається Адміністрацією Держспецзв'язку;

приміщення для роботи із замовниками послуг, зберігання обладнання, що забезпечує надання обраного виду послуг, обробки та зберігання документів, розроблених під час надання послуг згідно з ліцензією.

23. Програмні та інші вироби, що є об'єктами права інтелектуальної власності, повинні використовуватися ліцензіатом на підставі відповідного ліцензійного договору, укладеного з власником таких прав.

24. Провадження ліцензованої діяльності у галузі криптографічного захисту інформації здобувач ліцензії чи ліцензіат здійснює за умови:

укомплектованості обчислювальною, розмножувальною та організаційною технікою, відповідним програмним забезпеченням, необхідним для складення (створення) конструкторської та іншої технічної документації;

наявності інформаційного забезпечення для складення (створення) конструкторської та іншої технічної документації, можливості оперативного внесення змін і доповнень до такої документації, умов її обліку, збереження та ефективного контролю, який забезпечує комплектність конструкторської та іншої технічної документації, а також регламентує порядок доступу до неї;

забезпечення здійснення вхідного контролю за криптосистемами і засобами криптографічного захисту інформації, що підлягають монтажу та налаштуванню;

наявності системи технічного обслуговування та ремонту криптосистем і засобів криптографічного захисту інформації;

наявності засобів вимірювання, відповідних методик та інструкцій, необхідних для налаштування, перевірки встановлених параметрів та якості продукції і технологічних операцій;

здійснення монтажу (встановлення), налаштування, технічного обслуговування (супроводження) криптосистем і засобів криптографічного захисту інформації згідно з робочою конструкторською, експлуатаційною та нормативною документацією щодо криптосистем і засобів криптографічного захисту інформації.

25. Наявність у ліцензіата ліцензії на провадження ліцензованої

діяльності у галузі криптографічного захисту інформації, що становить державну таємницю, надає право на провадження ліцензованої діяльності у галузі криптографічного захисту службової інформації,

відкритої інформації, яка належить до державних інформаційних ресурсів, конфіденційної інформації, що передана її власником державі та обробляється в інформаційно-телекомунікаційних системах державних органів.

Наявність у ліцензіата ліцензії на провадження ліцензованої діяльності у галузі криптографічного захисту службової інформації надає право на провадження ліцензованої діяльності у галузі криптографічного захисту відкритої інформації, яка належить до державних інформаційних ресурсів, конфіденційної інформації, що передана її власником державі та обробляється в інформаційно-телекомунікаційних системах державних органів.

26. Для провадження ліцензованої діяльності у галузі криптографічного захисту інформації, що становить державну таємницю, здобувач ліцензії чи ліцензіат повинен мати:

спеціальний дозвіл на провадження діяльності, пов’язаної з державною таємницею. Зазначена в спеціальному дозволі категорія режиму секретності повинна відповідати ступеню секретності відомостей, використання яких передбачено за відповідним видом послуг;

спеціалістів, діяльність яких безпосередньо пов’язана з державною таємницею, з відповідними допусками до державної таємниці. Форма допусків повинна відповідати ступеню секретності відомостей, до яких такі спеціалісти допущені (передбачено їх допуск);

приміщення із створеними та атестованими щодо відповідності вимогам нормативних документів з технічного захисту інформації комплексами технічного захисту інформації, які облаштовані відповідно до вимог нормативно-правових актів з питань безпеки спеціального зв’язку;

технічні засоби обробки секретної інформації та/або інформаційні (автоматизовані) системи, в яких створено комплексну систему захисту інформації з підтвердженою відповідністю (в разі потреби).

27. Провадження ліцензованої діяльності у галузі криптографічного захисту інформації, що становить державну таємницю, здійснюється в межах строку дії спеціального дозволу на провадження діяльності, пов’язаної з державною таємницею, та допусків до державної таємниці працівників, діяльність яких безпосередньо пов’язана з державною таємницею.

28. Провадження ліцензованої діяльності у галузі криптографічного захисту інформації здійснюється згідно з режимом безпеки поводження із засобами криптографічного захисту службової інформації та інформації, що становить державну таємницю, нормативної та експлуатаційної документації до них.

Отже, ми докладно розглянули ліцензійні умови, у разі виконання яких суб'єкти господарської діяльності можуть отримати ліцензію та надавати послуги у галузі криптографічного захисту інформації.

Ліцензійні умови є конкретними, багатоплановими та досить жорсткими вимогами щодо умов, за виконанням та дотриманням яких може здійснюватися діяльність в галузі КЗІ. Процес отримання суб'єктами ліцензії на право займатися відповідною господарською діяльністю не є простою справою. Він потребує від суб'єктів точного та повного виконання всіх положень ліцензійних вимог, як на етапі отримання ліцензії, так і спрямовує усі технологічні процеси господарської діяльності в русло обов'язкового дотримання вимог чинних НПА в цій сфері протягом усього терміну дії ліцензії.

Таким чином, за результатом розгляду та аналізу положень наведених основних нормативно-правових актів України з криптографічного захисту інформації, можна зробити висновки щодо великого обсягу, багатовекторності, складності та жорсткої регламентації робіт у галузі КЗІ. Ці висновки обґрунтовують необхідність системного та поглибленого вивчення вимог НПА та нормативних документів інституційного рівня, чинних у галузі КЗІ, як теоретичного підґрунтя у формуванні необхідних професійних компетентностей майбутніх фахівців ДССЗЗІ.

3.2 Нормативно-правове забезпечення здійснення електронного документообігу в державі

Застосування технологій криптографічного захисту інформації є обов'язковим у разі, коли впроваджується електронний документообіг в установах. З'ясуємо нормативно-правове обґрунтування цього твердження.

Як було з'ясовано раніше, до категорій інформації, що підлягають обов'язковому захисту, належать:

службова та відкрита інформація, що є власністю держави, захист якою здійснюється відповідно до законодавства України;

персональні дані особи;

критична інформація;

інформація, яка містить відомості, що складають державну таємницю.

У цьому розділі навчального посібника предметом розгляду буде перша складова із вище вказаних категорій інформації, а саме *службова та відкрита інформація, що є власністю держави*.

З цією метою розглянемо наступну низку законодавчих та нормативно-правових актів України, положення яких складають правове

підґрунтя здійснення електронного документообігу в державних установах із використанням технологій криптографічного захисту відкритої інформації, яка є власністю держави, а саме:

Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851- IV, (зі змінами);

наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5 (зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198), яким введено в дію "Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання";

постанова Кабінету Міністрів України від 17 січня 2018 року № 55, якою введена в дію "Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну".

3.2.1 Закон України "Про електронні документи та електронний документообіг" від 22.05.2003 № 851- IV

Першим у переліку наведено ***Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, (зі змінами).*** *Саме він встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів у державі.* [54]

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України "Про інформацію", "Про захист інформації в інформаційно-комунікаційних системах", "Про державну таємницю", "Про електронні комунікації", "Про обов'язковий примірник документів", даним Законом, а також іншими нормативно-правовими актами держави.

Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003року № 851-IV, (зі змінами) складається із п'яти розділів: [54]

Розділ I Загальні положення (ст. ст. 1 – 4);

Розділ II Електронний документ (ст. ст. 5 – 8);

Розділ III Засади електронного документообігу (ст. ст. 9 – 13);

Розділ IV Організація електронного документообігу (ст. ст. 14 – 18);

Розділ V Прикінцеві положення.

В *Розділі І Загальні положення* наведені основні терміни, сфера дії закону, законодавство та основи державного регулювання електронного документообігу.

В *Розділі ІІ Електронний документ* наведено визначення поняття *“електронний документ”,* встановлено його обов’язкові реквізити та технології створення, а також засвідчено правовий статус електронного документа (його копії) на рівні документа, відпрацьованого на паперовому носії.

В цьому розділі особливу увагу необхідно приділити використанню *електронного (цифрового) підпису*, як технології криптографічного захисту інформації та важливого реквізиту, що завершує електронний документ, ідентифікує його автора, засвідчує його справжність та цілісність (ст. 6).

В *Розділі ІІІ Засади електронного документообігу* наведено визначення поняття *“електронний документообіг”* та встановлено порядок реалізації головних процесів документообігу: відправлення, передавання, одержання, перевірка цілісності, зберігання та архівування електронних документів.

Доцільно звернути особливу увагу та запам’ятати наступні положення цього розділу:

Ст. 9. ***Електронний документообіг*** *(обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів.*

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно із законодавством.

Ст. 10. Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ.

Датою і часом відправлення електронного документа вважаються дата і час здавання його для пересилання.

Ст. 11. Електронний документ вважається одержаним *адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа.* Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження.

Ст. 12. Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису документа.

Ст. 13. Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

В *Розділі IV Організація електронного документообігу* наведено головні організаційні засади електронного документообігу.

Доцільно особливу увагу звернути на наступні положення цього розділу:

Ст. 15. *В інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах, які забезпечують обмін електронними документами, що містять державні інформаційні ресурси, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства*.

Ст. 18. *Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.*

В *Розділі V Прикінцеві положення* сформульовані терміни набрання чинності положень Закону та надано доручення Кабінету Міністрів України протягом шести місяців з дня набрання ним чинності реалізувати низку заходів щодо вдосконалення системи нормативно-правових актів у галузі документоведення у відповідність до вимог даного Закону.

Отже, Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, (зі змінами) встановлює основні організаційно-правові засади електронного документообігу та закладає законодавчі основи створення нормативно-правового забезпечення у вигляді цілої низки НПА, які деталізують порядок реалізації обов'язкових процесів документообігу із забезпеченням захисту інформації (в тому числі й криптографічного захисту) на кожному із них.

Положення цього Закону передбачають дотримання порядку формування документів, організації та здійснення документообігу в установах, встановленого відповідними державними стандартами та інструкціями з документоведення. Вимоги стандартів та інструкцій

повинні виконуватися незалежно від того, в якому вигляді (паперовому або електронному) створені документи.

Цим обґрунтовується необхідність розгляду положень чинних в державі державних стандартів та інструкцій щодо документоведення в державних установах.

3.2.2 ДСТУ 4163:2020 "Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів". Чинні інструкції щодо документоведення в державних установах.

У статті 9 Розділу III Закону України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, (зі змінами) зроблено акцент на обов'язкове дотримання встановленого порядку реалізації усіх процесів документообігу, починаючи із процесу *створення документа*.

Цей процес є дуже важливим і це очевидний факт: якщо посадові особи не володіють знаннями та навичками створення документів, то весь процес управлінської діяльності в установі стає неможливим. Юридичної сили набувають тільки ті організаційно-розпорядчі документи, які санкціоновані (підписані, затверджені) керівником установи, а це може статись тільки за умов їх створення відповідно до вимог чинних у державі стандартів та інструкцій щодо документоведення. Ці вимоги є обов'язковими як для документів на паперових носіях, так і ОРД в електронному вигляді.

Із цього робимо *висновок, що знання посадовими особами вимог цих нормативно-правових документів є важливими та обов'язковими.*

Розглянемо основні положення цієї низки НПА.

Положення ДСТУ 4163:2020 "Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів"

Вимоги *ДСТУ 4163:2020 "Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів"* поширюються на *організаційно-розпорядчі документи незалежно від носія інформації* (далі – документи), зокрема на: організаційні (положення, статути, посадові інструкції, штатні розписи тощо); розпорядчі (постанови, рішення, накази, розпорядження); інформаційно-аналітичні (акти, довідки, доповідні записки, пояснювальні записки, службові листи тощо) документи, створювані в результаті діяльності державних органів, органів місцевого

самоврядування, установ, підприємств, організацій та інших юридичних осіб незалежно від їхнього функціонально-цільового призначення, рівня і масштабу діяльності та форми власності. [55]

Цей стандарт установлює: склад реквізитів документів; вимоги до змісту та місця розташування реквізитів у документах; вимоги до бланків та оформлення документів; вимоги до виготовлення документів.

Вимоги цього стандарту щодо оформлення реквізитів поширюються на всі класи уніфікованих систем документації.

Стандарт визначає склад і зміст постійної інформації реквізитів у кількості 32 для організаційно-розпорядчих документів незалежно від носія інформації, а саме:

01 – зображення Державного Герба України, Герба Автономної Республіки Крим;

02 – зображення емблеми юридичної особи або торговельної марки (знак для товарів і послуг);

03 – найменування юридичної особи вищого рівня;

04 – найменування юридичної особи;

05 – найменування структурного підрозділу юридичної особи;

06 – довідкові дані про юридичну особу;

07 – код форми документа;

08 – код юридичної особи;

09 – назва виду документа;

10 – дата документа;

11 – реєстраційний індекс документа;

12 – посилання на реєстраційний індекс і дату документа, на який дають відповідь;

13 – місце складення документа;

14 – гриф обмеження доступу до документа;

15 – адресат;

16 – гриф затвердження документа;

17 – резолюція (рішення керівника установи, щодо виконання вимог ОРД);

18 – відмітка про контроль;

19 – заголовок до тексту документа;

20 – текст документа;

21 – відмітка про наявність додатків;

22 – підпис;

23 – відбиток печатки;

24 – віза документа;

25 – гриф погодження (схвалення) документа;

26 – відмітка про засвідчення копії документа;

27 – відомості про виконавця документа;

28 – відмітка про ознайомлення з документом;

29 – відмітка про виконання документа;

30 – відмітка про надходження документа до юридичної особи;

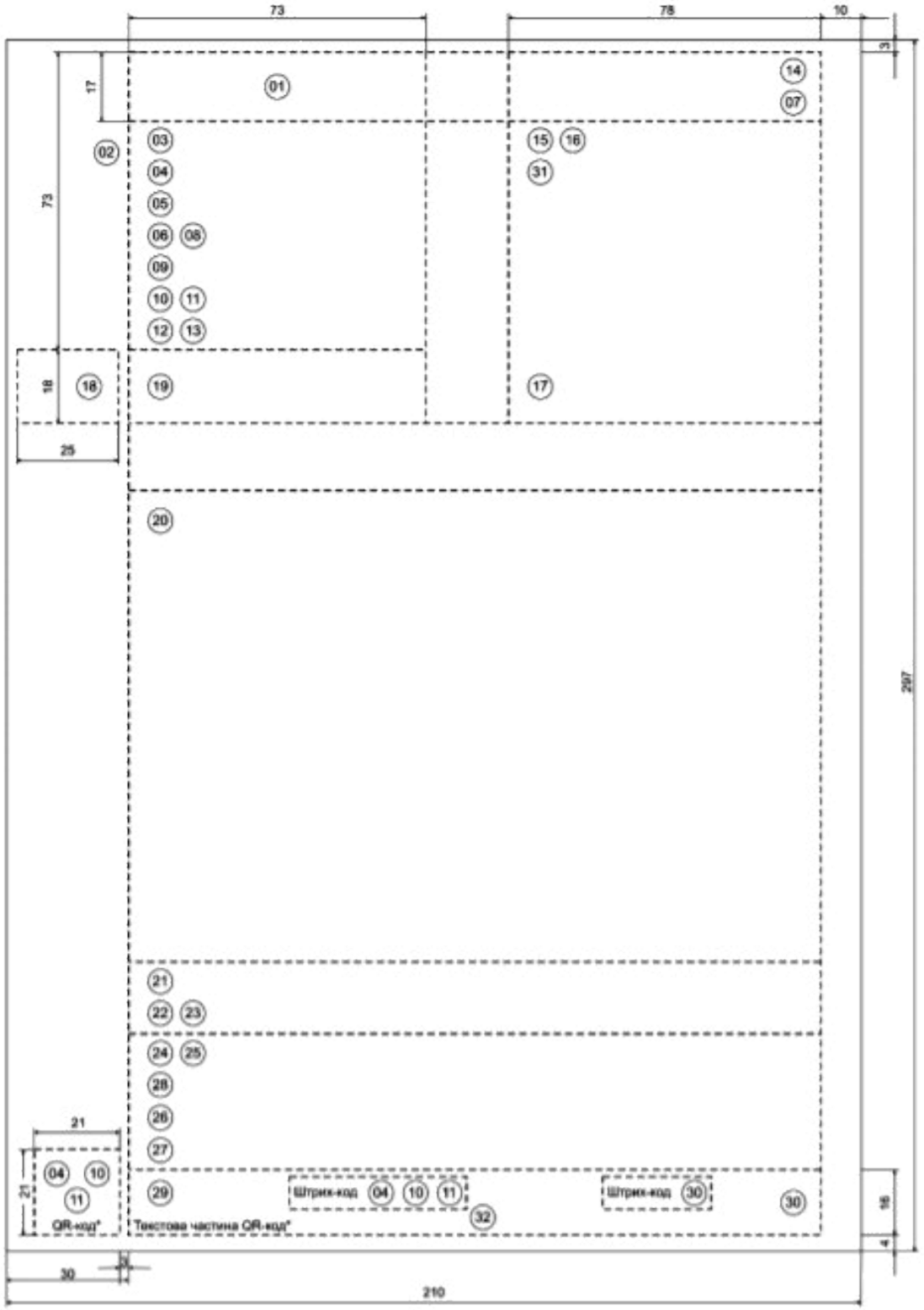
31 – запис про державну реєстрацію;

32 – відмітка про наявність примірника з паперовим (електронним) носієм інформації.

Схеми розташування реквізитів і меж зон на аркуші формату А4 кутового і поздовжнього бланка наведено в додатку А до стандарту (Рис. 3.1 А.1 та Рис. 3.1 А.2):

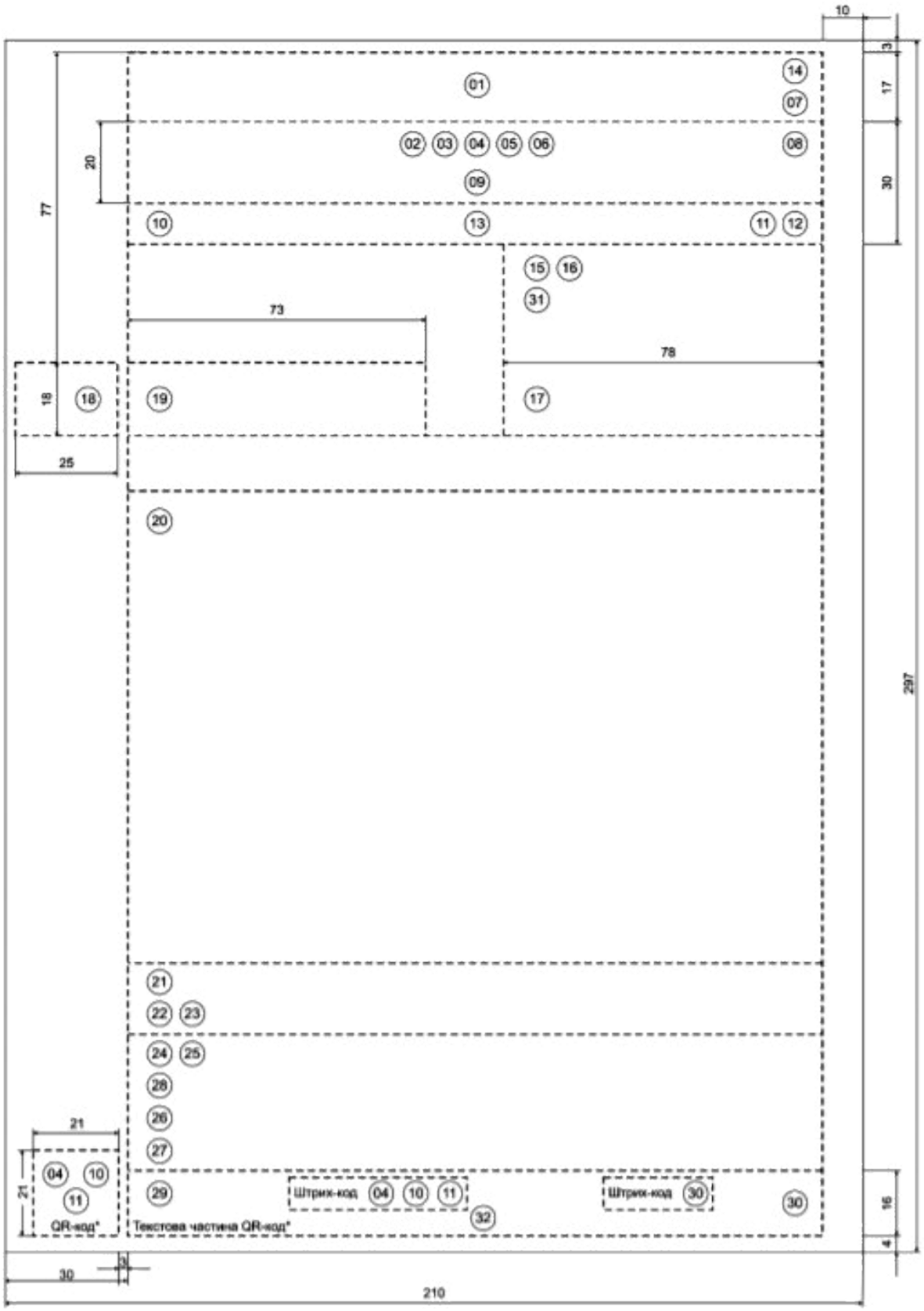
ДОДАТОК А

Схеми розташування реквізитів документів



* Відомості про підписувача електронного документа або накладача електронної печатки

Рис. 3.1 А.1 Схема розташування реквізитів і меж зон на форматі А4 кутового бланка



* Відомості про підписувача електронного документа або накладача електронної печатки

Рис. 3.1 А.2 Схема розташування реквізитів і меж зон на форматі А4 поздовжнього бланка

Організаційно-розпорядчі документи в установах повинні бути відпрацьовані згідно з вимогами Державного Стандарту та Схеми розташування реквізитів і меж зон на форматі А4, наведеної в ньому. Приклад документа (вхідний лист до юридичної особи) наведено нижче (Рис.3.2):

Товариство з обмеженою відповідальністю
«МотоЛюкс»
вул. Дачна, 134, офіс 2,
с. Копилів, Макарівський р-н,
Київська обл., 08033,
тел. (04567) 3 01 02
Код ЄДРПОУ 11511361

15.11.2019 № *23/01-10*

Державний архів Київської області
вул. Юрія Іллєнка, 38,
м. Київ, 04119,
тел. (044) 206 74 99

Про погодження номенклатури справ
ТОВ «МотоЛюкс»

Титаренко А.
Прошу до 07.12.2019 підготувати документи для розгляду на засіданні ЕПК архіву
Особистий підпис
20.11.2019

Інформуємо, що відповідно до рішення Установчих зборів засновників від 01.01.2019 створено Товариство з обмеженою відповідальністю «МотоЛюкс» (далі — ТОВ), яке зареєстровано 11.01.2018 реєстраційною службою Макарівського району Київської області (код ЄДРПОУ 12345678).

Відповідно до статті 32 Закону України «Про Національний архівний фонд України та архівні установи» надсилаємо на погодження номенклатуру справ товариства на 2020 рік.

За результатами розгляду номенклатури справ просимо письмово повідомити про внесення ТОВ до відповідного списку юридичних осіб, що перебувають у зоні комплектування архівного відділу.

Додатки: 1. Номенклатура справ на 5 арк. у 4 прим.
2. Копія статуту ТОВ «МотоЛюкс» на 10 арк. в 1 прим.

Директор Особистий підпис Володимир МОРОЗ

Примак Сергій (04567) 3 01 02

До справи № 01-23
Розглянуто на засіданні ЕПК архіву,
надіслано на доопрацювання
Секретар Особистий підпис Тетяна ДЗИҐА
09.12.2019

Держархів Київської обл.
Вх. № 213
20.11.2019

Рис. 3.2 Приклад оформлення вхідного листа до юридичної особи

Як бачимо, положення Державного Стандарту та Схема розташування реквізитів визначають повний їх перелік, вимоги щодо оформлення та місця розташування та матеріальному носієві.

Кожному виду організаційно-розпорядчого документа притаманні певні реквізити із наведеного повного переліку. Залежно від виду ОРД, притаманні йому реквізити мають бути оформленні відповідно до схеми розташування реквізитів та встановлених стандартом вимог. У ДСТУ встановлено вимоги щодо оформлення визначених реквізитів.

Отже, *ДСТУ 4163:2020 "Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів" за своїм головним призначенням є у певному сенсі еталоном загальних вимог щодо оформлення ОРД у державі, але він не може враховувати безліч особливостей щодо оформлення кожного із наявних видів ОРД (доповідні записки, розпорядження, накази, протоколи, директиви, донесення, звіти, тощо).*

З цією метою в державі ***постановою Кабінету Міністрів України від 17 січня 2018 року № 55 затверджена "Типова інструкція з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади"*** *(далі – Типова інструкція)***.**

Типова інструкція встановлює вимоги щодо документування управлінської інформації та організації роботи з документами, створеними у паперовій формі Секретаріатом Кабінету Міністрів України, центральними органами виконавчої влади, їхніми територіальними органами, Радою міністрів Автономної Республіки Крим, місцевими органами виконавчої влади, підприємствами, установами, організаціями, що належать до сфери управління центральних або місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим (далі – установи). [56]

В її положеннях сформульовано вимоги щодо особливостей оформлювання певних видів ОРД у паперовій формі.

Так, у розділі ***Складення деяких видів документів*** деталізовано вимоги щодо оформлювання:

– *наказів (розпоряджень*) у п.п. 80 – 105;
– *протоколів* у п.п. 106 – 122;
– *службових листів* у п.п. 123 – 130;
– *інших видів ОРД* у п.п. 131 – 144.

В *Типовій інструкції* встановлено послідовність виконання усіх процесів, пов'язаних із створенням ОРД та їх подальшим документообігом

від надавача до адресата, а після завершення термінів зберігання – передачі до архівних установ.

На підставі положень ДСТУ 4163:2020, “Типової інструкції з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади”, а також враховуючи специфіку функціонування її структурних органів, в ДССЗЗІ України відпрацьовано та наказом Адміністрації Держспецзв’язку України від 29 лютого 2012 року № 100 введено в дію *“Інструкцію з організації діловодства в Державній службі спеціального зв’язку та захисту інформації України”*, зі змінами.

Цей галузевий нормативний документ складається із 9 розділів та 29 додатків. Текстуальна частина нормативного документа за змістом максимально наближена до змісту попередніх НПА. Додатки містять зразки форм документів, а також окремі положення, які враховують специфіку функціонування установ ДССЗЗІ України.

Зрозуміло, що посадові особи установ ДССЗЗІ України зобов’язані досконало знати положення вищевказаних НПА та володіти практичними навичками виконання їх вимог під час здійснення процедур документоведення.

Отже, положення ДСТУ 4163:2020 “Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів”, “Типової інструкції з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади” (затвердженої постановою Кабінету Міністрів України від 17 січня 2018 року № 55), галузевої “Інструкції з організації діловодства в Державній службі спеціального зв’язку та захисту інформації України” введеної в дію наказом Адміністрації Держспецзв’язку України від 29 лютого 2012 року № 100 є базовими, вони встановлюють вимоги щодо документування управлінської інформації та організації роботи з документами, створеними в паперовій формі. Ці вимоги є обов’язковими також і в здійсненні електронного документообігу в установах ДССЗЗІ України.

Особливості роботи з електронними документами в установах України розглянемо у наступному підпункті.

3.2.3 “Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11.11.2014 № 1886/5, зареєстровано в Міністерстві юстиції України 11.11.2014 за № 1421/26198)

“Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198), який встановлює загальні вимоги щодо впровадження електронного документообігу із застосуванням кваліфікованого електронного підпису чи печатки, організації роботи з електронними документами у діловодствах державних органів, органів місцевого самоврядування, підприємств, установ та організацій незалежно від форм власності (далі – установ) та щодо їх підготовки до передавання на архівне зберігання.

Докладно розглянемо та з'ясуємо положення цього важливого НПА України.

Вимоги цього *Порядку є* обов'язковими для виконання державними органами, підприємствами, установами і організаціями незалежно від форм власності (далі – організації), в яких упроваджено та здійснюється електронний документообіг.

Структура змісту Порядку: [57]

Зміст складається із *9 розділів*:

Розділ I – Загальні положення

Розділ II – Підготовка та оформлення електронних документів:

1. Вимоги до створення електронних документів.

2. Технологічні особливості оформлення реквізитів організаційно-розпорядчих електронних документів.

3. Зберігання та склад реквізитів електронних документів.

4. Створення електронного документа.

5. Конвертування електронних документів.

6. Створення XML-документа.

Розділ III – Організація електронного документообігу та виконання документів:

1. Вимоги до електронного документообігу.

2. Вимоги до уніфікації інформаційних об’єктів електронного документообігу.

3. Доставка електронних документів.

4. Технічна перевірка вхідного електронного документа.

5. Технічна перевірка файлу XML-документа.

6. Технічна перевірка електронних документів, що містяться в XML-документі.

7. Електронне повідомлення про доставку / отримання / реєстрацію / відмову в реєстрації електронного документа адресатом вхідного електронного документа.

8. Попередній розгляд електронних документів.

9. Реєстрація електронних документів.

10. Організація проходження електронних документів та їх виконання.

11. Організація контролю за виконанням електронних документів.

12. Порядок надсилання вихідних електронних документів.

13. Повторне надсилання відхиленого вхідного електронного документа.

14. Інформаційно-довідкова робота з електронними документами.

Розділ IV – Систематизація та зберігання електронних документів у діловодстві:

1. Зберігання електронних документів в установі.

2. Зберігання вхідних електронних документів.

3. Підготовка та оформлення електронних документів до оперативного зберігання.

4. Організація доступу до електронних документів в установі.

5. Складання номенклатури справ.

6. Створення засвідченої паперової копії електронного документа.

7. Формування та оформлення електронних справ в структурних підрозділах установи.

Розділ V – Підготовка справ до передавання на архівне зберігання:

1. Експертиза цінності електронних документів.

2. Складання та оформлення описів справ у діловодстві установи.

3. Передавання справ до архіву установи.

Розділ VI – Знищення електронних документів.

Розділ VII – Особливості організації роботи з електронними документами в архіві установи:

1. Складання і оформлення річних розділів описів справ постійного зберігання.

2. Створення архівних електронних документів.

3. Створення та оформлення архівних електронних справ.

4. Створення та оформлення обкладинки архівної електронної справи.

5. Створення та оформлення внутрішніх описів документів справ.

Розділ VIII – Підготовка електронних документів Національного архівного фонду до передавання на постійне зберігання.

Розділ IX – Технічні вимоги до автоматизованого робочого місця працівника архіву установи.

Після змісту розділів в *Порядку* розміщено 17 Додатків. Кожний із додатків є зразком відповідного документу або форми певного облікового журналу (бланку, опису), які використовуються під час здійснення відповідних процесів електронного документообігу *(докладно можна ознайомитись під час самостійної роботи)*.

Із аналізу структури змісту даного НПА вже стає зрозумілим, що документ деталізує кожний процес електронного документообігу, складає не тільки правове підґрунтя для обов'язкового виконання, а й встановлює порядок практичної реалізації кожного із його процесів.

В цьому розділі посібника ми не ставимо перед собою мету щодо детального вивчення вимог усіх розділів Порядку, *які містяться на 46 сторінках формату А4 у шрифті 12. Наша мета – з'ясувати головні положення НПА, що складають правове підґрунтя здійснення електронного документообігу в державних установах із використанням технологій криптографічного захисту інформації, яка є власністю держави, починаючи з відкритої інформації управлінської діяльності установ.*

У цьому контексті доцільно звернути особливу увагу на наступні положення даного НПА: [59]

у розділі I – Загальні положення:

п. 1. Установи, в яких впроваджено системи електронного документообігу, *застосовують кваліфікований* ***електронний підпис чи печатку*** *відповідно до наказу Міністерства цифрової трансформації України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України* від 30 вересня 2020 року № 140/614 «Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг», зареєстрованого в Міністерстві юстиції України 22 жовтня 2020 року за № 1039/35322.

Удосконалені та інші види електронних підписів в електронному документообігу можуть застосовуватись установами для роботи з документами тимчасових строків зберігання відповідно до вимог статті 6 Закону України «Про електронні документи та електронний документообіг» з урахуванням загальних принципів роботи з електронними документами, встановлених цим Порядком.

У разі коли для документа, на який накладено удосконалений чи інший вид електронного підпису, за результатами проведеної експертизи цінності визначено постійний або тривалий (понад 10 років) строк зберігання, працівник архівного підрозділу або особа, відповідальна за ведення архіву установи, *засвідчує його* ***кваліфікованим електронним підписом***.

Визначення головних термінів, вжитих в цьому пункті НПА:

Електронний цифровий підпис *– вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа*.

Засіб кваліфікованого електронного підпису чи печатки *– апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам Закону.*

п.п. 8 та 9. Технічні вимоги до інформаційної автоматизованої системи (*далі – ІАС*) та окремих технічних і програмних засобів, призначених для організації електронного документообігу, та порядок їх упровадження здійснюються відповідно до чинного законодавства.

Питання вибору технологій та реалізації процесів в ІАС, що забезпечують виконання вимог цього Порядку, вирішуються під час розроблення технічного завдання на створення конкретної ІАС або її модернізації.

Захист інформації в АС установи забезпечується відповідно до вимог Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», інших нормативно-правових актів у сфері захисту інформації.

п. 11. Технічне супроводження електронного документообігу в установі та його програмно-апаратне забезпечення покладаються *на структурний підрозділ (департамент, управління, відділ, сектор) з питань інформаційного забезпечення (інформаційних технологій) або фахівця з інформаційних технологій,* на якого покладається виконання завдань і

функцій структурного підрозділу з питань інформаційного забезпечення (далі – служба інформаційних технологій).

Контроль за станом захищеності інформації*, що обробляється в ІАС установи, покладається на структурний підрозділ (департамент, управління, відділ, сектор) з питань захисту інформації або фахівця із захисту інформації, на якого покладається виконання завдань і функцій структурного підрозділу з питань захисту інформації.*

Як бачимо, в перших пунктах *Загальних положень* даного НПА встановлено вимоги щодо *обов'язковості захисту відкритої інформації управлінської діяльності із використанням таких технологій криптографічного захисту інформації як електронний цифровий підпис (більш сучасніший термін – кваліфікований електронний підпис), а також вимоги щодо дотримання правил захисту інформації, яка підлягає обробці, відповідно до чинного законодавства держави.*

у розділі ІІ – Підготовка та оформлення електронних документів:
1. Вимоги до створення електронних документів:

п. 2, п. 3. Електронний документ має бути оформлений за загальними правилами документування і мати реквізити, що встановлені для аналогічного документа у паперовій формі.

Оформлення реквізитів організаційно-розпорядчих електронних документів здійснюється електронними засобами документування інформації з урахуванням вимог *Національного стандарту України ДСТУ 4163-2020 «Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів»,* затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 01 липня 2020 року № 144.

Створення деяких реквізитів електронного документа, наведених у пунктах 1 – 10 глави 2 цього розділу, здійснюється за технологією, що відрізняється від створення відповідних реквізитів для документів у паперовій формі.

Необхідно звернути увагу на те, що не зважаючи на єдині вимоги ДСТУ 4163-2020 щодо оформлення документів на паперових носіях та в електронному вигляді, *існують певні особливості у технологіях створення окремих реквізитів під час формування електронних документів*. Такі особливості потребують знання та виконання відповідних пунктів *Порядку* посадовими особами установ.

У главі 3. Доставка електронних документів розділу ІІ:

Заслуговує *уваги обов'язковість здійснення моніторингу безпеки АС та перевірки автентичності електронних документів під час їх отримання.*

Так, в п. 3 даної глави зазначається:

Для забезпечення безпеки АС установи приймання та технічна перевірка електронних документів здійснюються за допомогою відокремленої від основної ІАС автоматизованої системи зі створеною в її складі комплексною системою захисту інформації з підтвердженою відповідністю у встановленому законодавством України порядку.

Далі у главах 4 – 6 даного розділу визначений порядок здійснення такої технічної перевірки отриманих електронних надходжень.

В главі 7 розділу ІІ встановлено вимоги щодо обов'язковості направлення на адресу відправника електронного повідомлення про доставку / отримання / реєстрацію / відмову в реєстрації електронного документа адресатом вхідного електронного документа.

Так, в п. 1 даної глави визначено:

Після технічної перевірки вхідного електронного документа працівником служби діловодства, відповідальним за опрацювання вхідних електронних документів, створюється електронне повідомлення про доставку / отримання / реєстрацію / відмову в реєстрації електронного документа адресатом цього електронного документа, яке надсилається його відправнику (автору).

Ці дії є важливою складовою у контролі проходження документів від відправника до отримувача із дотриманням гарантій їхньої автентичності та цілісності.

В главі 10 розділу ІІ Організація проходження електронних документів та їх виконання особливої уваги заслуговує *обов'язкова процедура обмеження кола посадових осіб установи, які мають повноваження накладання кваліфікованого електронного підпису чи печатки* (отримання необхідних засобів кваліфікованого електронного підпису чи печатки).

Так, в п. 2 даної глави зазначено:

Відповідно до схем проходження електронних документів, затверджених керівником установи, визначається та затверджується список посадових осіб, які мають отримати необхідні засоби кваліфікованого електронного підпису чи печатки для накладання кваліфікованого електронного підпису чи печатки установи.

В процесі уважного вивчення положень інших глав та розділів даного НПА подібні вимоги щодо забезпечення безпеки інформації з управлінської діяльності в електронній формі в діловодствах установ держави. Одним із важливих складових СБІ є застосування технологій криптографічного захисту інформації, підсилених цілою низкою організаційних та організаційно-технічних заходів захисту.

Отже, "Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання" (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198), встановлює загальні вимоги щодо впровадження електронного документообігу та організації роботи з електронними документами у діловодствах установ держави.

Виконання цих вимог забезпечує безпеку відкритої інформації з управлінської діяльності в електронній формі і є обов'язковими для державних органів, органів місцевого самоврядування, підприємств, установ та організацій незалежно від форм власності.

3.2.4 "Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (постанова КМУ від 17.01.2018 № 55)

Наступним НПА цього ж ієрархічного рівня є *"Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (постанова КМУ від 17 січня 2018 року № 55)*.

Вимоги цієї *Інструкції* базуються на положеннях_Закону України "Про електронні документи та електронний документообіг", "Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання" (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198) та інших актів законодавства України.

Положення *Інструкції* поширюється на всі електронні документи, що створюються, відправляються або одержуються Секретаріатом Кабінету Міністрів України, центральними органами виконавчої влади, їхніми територіальними органами, місцевими органами виконавчої влади, підприємствами, установами, організаціями, що належать до сфери

управління центральних або місцевих органів виконавчої влади *(далі – установи)*. [58]

Головною особливістю цього НПА є те, що за видом він належить до категорії – *"інструкція"*.

За визначенням *"інструкція" – це документ, у якому викладають правила, що регулюють спеціальні сторони діяльності і стосунки установ чи поведінку працівників ід час виконання службових обов'язків; це зведення правил, детальні настанови, приписи керівного органу підпорядкованим органам, які є обов'язковими для виконання.*

Текст даного НПА повністю відповідає категорії "інструкція" та містить покрокові послідовні детальні настанови та приписи щодо:

організації проходження електронного документа з моменту його створення або одержання і до моменту відправлення (передавання) до архівного підрозділу установи;

забезпечення функціонування та використання системи електронної взаємодії органів виконавчої влади ;

організації оперативного інформаційного обміну з використанням службової електронної пошти.

здійснення моніторингу стану виконання управлінських рішень.

Інструкція складається із текстової частини та Додатків 1 – 9. [60]

Текстова частина *Інструкції* у обсязі 217 пунктів, складається із 7 розділів:

Розділ I – Загальні положення (п. 1 – п. 13).

Розділ II – Міжвідомчий обмін електронними документами (п. 14 – п. 33):

Приймання вхідних електронних документів.

Надсилання вихідних електронних документів.

Журнал обміну електронних документів.

Особливості електронної взаємодії без застосування системи взаємодії.

Розділ III – Організація електронного документообігу (п. 34 – п. 73):

Облік обсягу електронного документообігу.

Реєстрація документів.

Організація передавання документів та визначення їх виконавців.

Розділ IV – Документування управлінської інформації в електронній формі (п. 74 – п. 161):

Загальні вимоги до створення документів.

Підготовка проєктів електронних документів.
Особливості підготовки деяких видів електронних документів.

Розділ V – Моніторинг за станом виконання управлінських рішень (п. 162 – п. 179).

Розділ VI – Систематизація та зберігання документів у діловодстві (п. 180 – п. 200):
Складення номенклатури справ.
Формування електронних справ.
Зберігання електронних документів в установах.

Розділ VII – Порядок підготовки електронних справ до передавання для архівного зберігання (п. 201 – п. 217):
Експертиза цінності документів.
Оформлення електронних справ.
Передавання електронних справ до архівного підрозділу установи.

Після змісту розділів в Інструкції розміщено 9 Додатків. Кожний із додатків є зразком відповідного документа або форми певного облікового журналу (бланку, опису), які використовуються під час здійснення відповідних процесів електронного документообігу.

(Доцільно здобувачам вищої освіти під час самостійної роботи докладно попрацювати зі змістом та додатками цього НПА).

Структура змісту даного НПА, логічна послідовність викладання вимог та ступінь деталізації кожного процесу електронного документообігу надає можливість посадовим особам установ практично їх упроваджувати в установах.

Окрім цього, на підставі положень цієї Інструкції установи з врахуванням особливостей та специфіки їхньої діяльності розробляють *власні інструкції з діловодства* та організовують роботи з електронними документами на підставі власної інструкції. У змісті власних інструкцій з діловодства установ робиться відповідний акцент на обов'язковому та ретельному виконанні вище розглянутих технологій криптографічного захисту інформації.

Отже, в Україні створена система нормативно-правового забезпечення упровадження в установах держави електронного документообігу із використанням технологій криптографічного захисту відкритої інформації, яка є власністю держави.

Застосування технологій криптографічного захисту інформації в установах державі є обов'язковою.

Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 року № 851-IV, (зі змінами) встановлює основні організаційно-правові засади електронного документообігу та закладає законодавчі основи створення нормативно-правового забезпечення у вигляді цілої низки НПА, які деталізують порядок реалізації обов'язкових процесів документообігу із забезпеченням захисту інформації (в тому числі й криптографічного захисту) на кожному із них.

Вимоги цього Закону передбачають дотримання порядку формування документів, організації та здійснення документообігу в установах, встановленого відповідними державними стандартами та інструкціями з документоведення. Вимоги стандартів та інструкцій повинні виконуватись незалежно від того, в якому вигляді (паперовому або електронному) створені документи.

Положення ДСТУ 4163:2020 "Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів", "Типової інструкції з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади" (затвердженої постановою Кабінету Міністрів України від 17 січня 2018 року № 55), галузевої "Інструкції з організації діловодства в Державній службі спеціального зв'язку та захисту інформації України", введеної в дію наказом Адміністрації Держспецзв'язку України від 29 лютого 2012 року № 100, є базовими, вони встановлюють вимоги щодо документування управлінської інформації та організації роботи з документами, створеними у паперовій формі. Ці вимоги є обов'язковими також і в здійсненні електронного документообігу в установах ДССЗЗІ України.

"Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання" (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198), "Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (постанова КМУ від 17 січня 2018 року № 55) встановлюють вимоги щодо впровадження електронного документообігу та організації роботи з електронними документами у діловодствах установ держави.

Виконання цих вимог забезпечує безпеку відкритої інформації, що є власністю держави, в електронній формі і є обов'язковими для державних органів, органів місцевого самоврядування, підприємств, установ та організацій незалежно від форм власності.

3.3 Методичні рекомендації щодо вивчення положень основних законодавчих та нормативно-правових документів стосовно забезпечення використання електронних довірчих послуг у державі

Із положень попередніх пунктів даного розділу відомо, що в разі, коли установи здійснюють електронний документообіг, то відповідно до вимог чинних законодавчих та нормативно-правових актів України вони повинні обов'язково виконувати вимоги щодо захисту інформації управлінської діяльності із використанням таких технологій криптографічного захисту інформації як *кваліфікований електронний підпис, у поєднанні з комплексом організаційних та організаційно-технічних заходів захисту.*

У даному пункті розділу надано методичні рекомендації щодо самостійного вивчення здобувачами вищої освіти під час практичних (групових) занять положень основних законодавчих та нормативно-правових документів, які регламентують порядок використання електронних довірчих послуг в установах держави із ретельним дотриманням технологій криптографічного захисту інформації.

Щодо розуміння взагалі, про що йтиметься, необхідно з'ясувати суть терміна *"електронна довірча послуга"* та ті сфери суспільних відносин, яких він безпосередньо стосується.

Визначення: ***"електронна довірча послуга"*** *– послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги.*

Про неї доречно вести мову у випадках, коли суб'єкти інформаційних відносин вирішують певні завдання з використанням сучасних інформаційних технологій, пов'язаних з обробкою інформації з обмеженим доступом (персональні дані фізичних та юридичних осіб, інформація про фінансові перерахування клієнтів, характеристики об'єктів нерухомості та дані про їхніх власників у нотаріальному супроводженні закріплення права власності тощо). Сучасні технології електронної комунікації передбачають обов'язкові процедури ідентифікації користувачів та суб'єктів, які надають певні послуги, встановлення взаємної довіри, забезпечення цілісності та конфіденційності інформації в процесі розв'язання завдань.

Прикладами такої комунікації суб'єктів можуть бути:

здійснення фінансових операцій клієнтами через мобільні додатки банківських установ;

надання адміністративних послуг населенню державними установами через додаток Дія;

здійснення уповноваженими установами нотаріальних дій з використанням кваліфікованого електронного підпису;

використання громадянами системи електронної пошти в мережі Інтернет;

використання громадянами системи електронного спілкування із сімейним лікарем та медичними установами;

використання громадянами систем електронного спілкування з територіальними органами внутрішніх справ;

цей логічний ряд можемо продовжувати далі.

Вектор прикладання інтелектуальних зусиль під час роботи з наступною низкою законодавчих та НПА держави буде спрямований на з'ясування їхньої ієрархії та головних положень, які регламентують порядок надання відповідними установами електронних довірчих послуг із забезпеченням надійного захисту персональних даних суб'єктів правових відносин.

3.3.1 Методичні рекомендації щодо вивчення положень Закону України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII (зі змінами)

Закон України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII (зі змінами), очолює ієрархію НПА у цьому секторі ІБ.

Цей Закон визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов'язки суб'єктів відносин у сферах електронної ідентифікації та електронних довірчих послуг, порядок здійснення державного контролю за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг. [59]

Метою цього Закону є врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації.

Рекомендовано вивчення положень Закону здобувачами здійснити під керівництвом викладача під час практичного (групового) заняття в такій послідовності:

– викладач надає завдання курсантам щодо самостійного опрацювання положень законодавчого акту;

– здобувачі вищої освіти відповідно до отриманих завдань вивчають його.

Обсяг завдань щодо вивчення положень ***Закону України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII (зі змінами):***

– ознайомитись із структурою змісту Закону, порядком викладення положень Закону за розділами;

– опрацювати Розділи I – V Закону, особливу увагу звернути на положення таких статей закону: ст. ст. 2, 5, 8, 11 – 19, 32 – 35;

– під час роботи особливу увагу звернути на реалізацію технологій криптографічного захисту персональних даних суб'єктів інформаційних відносин держави.

Час на роботу з даним законодавчим документом – 40 хвилин.

Під час роботи здобувачів вищої освіти викладач контролює вивчення ними головних положень Закону, задає контрольні питання, оцінює відповіді здобувачів вищої освіти.

Контрольні питання та завдання:

1. *Доповісти про сферу дії Закону (Розділ 1 ст. 2).*
2. *Доповісти про основні принципи державного регулювання у сфері електронних довірчих послуг (Розділ 1 ст. 4).*
3. *Які органи здійснюють державне регулювання у сфері електронних довірчих послуг (Розділ I1 ст. 5)?*
4. *Доповісти про повноваження спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації (Розділ II ст. 8).*
5. *Доповісти про перелік суб'єктів відносин у сфері електронних довірчих послуг (Розділ II ст. 11).*
6. *Доповісти про права та обов'язки користувачів електронних довірчих послуг (Розділ II ст. 12).*
7. *Доповісти про права та обов'язки надавачів електронних довірчих послуг (Розділ II ст. 13).*
8. *Що являють собою засоби електронної ідентифікації, вимоги до них (Розділ III ст. 14)?*
9. *Які рівні довіри до засобів електронної ідентифікації може встановлювати схема електронної ідентифікації, що означає кожен із рівнів (Розділ III ст. 15)?*
10. *Які послуги входять до складу електронних довірчих послуг (Розділ 1V ст. 16)?*

11. *Кому надається та який порядок реалізації кваліфікованої електронної довірчої послуги (Розділ 1V ст. 18)?*
12. *Які вимоги встановлені до засобів кваліфікованого електронного підпису чи печатки (Розділ 1V ст. 19)?*
13. *Який орган та в якому порядку здійснює державний нагляд (контроль) за дотриманням вимог законодавства у сфері електронних довірчих послуг (Розділ V ст. 33)?*
14. *Яким порядком реалізується щорічна звітність контролюючого органу про оцінку діяльності суб'єктів відносин у сфері електронних довірчих послуг щодо дотримання вимог законодавства (Розділ V ст. 33 останній абзац)?*

Отже, *Закон України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII (зі змінами) є головним законодавчим актом держави, що визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг (в тому числі й ДССЗЗІ України), порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг.*

3.3.2 Методичні рекомендації щодо вивчення положень "Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності" (введено в дію постановою КМУ від 01 серпня 2023 року № 798)

"Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності" (введено в дію постановою КМУ від 01 серпня 2023 року № 798) *визначає вимоги щодо використання кваліфікованих електронних довірчих послуг в державних установах із врахуванням положень деяких законодавчих актів України щодо забезпечення укладення угоди між Україною та Європейським Союзом про взаємне визнання кваліфікованих електронних довірчих послуг та імплементації законодавства Європейського Союзу у сфері електронної ідентифікації.* [60]

Обсяг завдань щодо роботи із ***"Порядком використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями***

державної форми власності" (постанова КМУ від 01 серпня 2023 року № 798):

– опрацювати НПА у повному обсязі; особливу увагу звернути на положення таких пунктів НПА: п. п. 3 – 11, 13;

– під час роботи особливу увагу звернути на положення пунктів 3 – 11, 13 НПА, обов'язковості виконання технологій криптографічного захисту інформації, зобов'язань України перед країнами Європейського Союзу щодо гарантій безпеки надання кваліфікованих електронних довірчих послуг та імплементації законодавства ЄС у сфері електронної ідентифікації.

Час на роботу з даним НПА – до 40 хвилин.

Під час роботи здобувачів вищої освіти викладач контролює вивчення ними головних положень вказаного НПА, задає контрольні питання, оцінює відповіді.

Контрольні питання:

1. *Які кваліфіковані електронні довірчі послуги отримує державна установа (п. 3)?*
2. *Що використовують державні установи та їх працівники для засвідчення чинності відкритого ключа (п. 4)?*
3. *На кого покладаються завдання з організації використання кваліфікованих електронних довірчих послуг в установі, доповісти його функції (п. 6)?*
4. *Яке призначення кваліфікованої електронної печатки (п. 10)?*
5. *Який орган здійснює державний нагляд (контроль) за дотриманням у державних установах вимог цього Порядку (п. 13)?*

Отже, положеннями *"Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності" (постанова КМУ від 01.08.2023 № 798) з урахуванням положень НПА держав Євросоюзу конкретизовано вимоги щодо порядку використання кваліфікованих електронних довірчих послуг в державних установах.*

Отже, на аудиторних заняттях та під час самостійної роботи здобувачів вищої освіти доцільно вивчити положення наведених вище базових законодавчих та нормативно-правових актів, з'ясувати їхнє призначення, сферу застосування та місце кожного НПА у загальній ієрархії нормативно-правового забезпечення держави, яким регламентовано порядок використання електронних довірчих послуг в установах держави, а також вивчили їх головні положення для подальшого використання отриманих знань у професійній діяльності.

3.4. Методичні рекомендації щодо вивчення положень основних законодавчих та нормативно-правових документів щодо забезпечення державної експертизи у сфері криптографічного захисту інформації

Із матеріалу попередніх пунктів розділу 3 відомо, що у разі, коли у інформаційних відносинах суб'єктів держави використовуються електронні довірчі послуги, то одними із найголовніших вимог чинних НПА є *чітке виконання вставленого порядку їх надання, а також забезпечення необхідного рівня захисту інформації, що підлягає обробці, в результаті використання технологій КЗІ*.

Щодо надійності криптографічного захисту інформації, які реалізовані у технологіях надання кваліфікованих електронних довірчих послуг, виникає припущення (проводячи аналогію із засобами технічного захисту інформації) щодо обов'язковості проходження цими технологіями та відповідними засобами, що їх реалізують, експертизи (дослідження їх відповідності вимогам НПА) на державному рівні.

Головною метою вивчення здобувачами вищої освіти положень основних законодавчих та нормативно-правових документів щодо забезпечення державної експертизи у сфері криптографічного захисту інформації є набуття необхідних знань з цих питань, в результаті чого певні попередні припущення повинні перетворитись у переконання щодо обов'язковості та суворого порядку проходження технологіями та засобами криптографічного захисту інформації державної експертизи. Тільки за умов успішного проходження державної експертизи вони можуть бути застосовані установами держави.

Доцільно вивчення здобувачами вищої освіти вимог нормативно-правового забезпечення держави у цьому секторі здійснити під керівництвом викладача у ході практичного (групового) заняття, а також під час самостійної роботи в нижче наведеному порядку.

3.4.1 Методичні рекомендації щодо вивчення вимог "Положення про державну експертизу у сфері криптографічного захисту інформації" (наказ Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрований в Міністерстві юстиції України 16 липня 2008 року за № 651/15342)

"Положення про державну експертизу у сфері криптографічного захисту інформації" (наказ Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрований в Міністерстві юстиції України 16 липня 2008 року за № 651/15342) установлює порядок організації та

проведення державної експертизи у сфері криптографічного захисту інформації в Україні. [61]

Вивчення вимог цього *Положення* здійснюється в такій послідовності:

– викладач надає завдання курсантам щодо самостійного опрацювання положень НПА:

ознайомитись із структурою та порядком викладення положень змісту НПА та додатків до нього;

опрацювати зміст НПА у повному обсязі, особливу увагу звернути на положення таких пунктів: п. п. 1.3 – 1.13, 2.3.1 – 2.3.15.

– здобувачі вищої освіти відповідно до отриманих завдань вивчають положення НПА.

Час на роботу з даним НПА – 40 хвилин.

Пі час роботи здобувачів вищої освіти викладач контролює вивчення ними головних положень НПА, задає контрольні питання, оцінює відповіді.

Контрольні питання та завдання:

1. *Доповісти про сферу дії НПА, яке відношення його вимоги мають до фахівців Адміністрації Держспецзв'язку (Розділ 1 за сукупністю змісту всіх пунктів)?*
2. *Надати визначення поняттю "державна експертиза у сфері КЗІ (далі – експертиза)" (Розділ 1 п. 1.3).*
3. *Доповісти про перелік суб'єктів експертизи (Розділ І п. 1.4).*
4. *Що може бути об'єктом експертизи (Розділ І п. 1.5)?*
5. *Що є об'єктом обов'язкової експертизи (Розділ І п. 1.6)?*
6. *Які суб'єкти експертизи та на яких підставах здійснюють експертні (тематичні) дослідження (Розділ І п. 1.9)?*
7. *Які завдання покладаються на Експертну комісію Адміністрації Держспецзв'язку (Розділ І п. 1.10 – 1.13)?*
8. *Які документи суб'єктами надаються в Адміністрацію Держспецзв'язку для проведення експертизи засобів та систем генерації, тестування і розподілу ключових даних (Розділ ІІ за сукупністю відомостей п. п. 2.1.1 – п. 2.1.7)?*
9. *Доповісти про порядок проведення експертизи (Розділ ІІ п. 2.3.1 – 2.3.11).*
10. *У якому порядку документуються результати проведеної експертизи, які відомості повинні бути задокументовані (Розділ 1І п. п. 2.3.11 – 2.3.15)?*
11. *Які можуть бути підстави для анулювання експертного висновку (Розділ 1І п. п. 2.3.20 – 2.3.22)?*

Отже, *вимогами "Положення про державну експертизу у сфері криптографічного захисту інформації", введеного в дію наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрованого в Міністерстві юстиції України 16 липня 2008 року за № 651/15342, в редакції 2020 року установлено порядок організації та проведення державної експертизи у сфері криптографічного захисту інформації в Україні. Аналіз змісту цього НПА показує, що за загальною концепцією проведення державної експертизи у сфері криптографічного захисту інформації він дуже схожий на державну експертизу у сфері ТЗІ, але є й певні відмінності.*

Фахівці Держспецзв'язку, які задіяні у реалізації заходів державної експертизи, повинні докладно знати положення даного НПА та формувати практичні вміння їх застосування для виконання своїх функціональних обов'язків.

3.4.2 Порядок проведення державної експертизи. Експертний висновок

Положення попереднього НПА розглядаються та обговорюються під керівництвом викладача за активної участі здобувачів вищої освіти.

Вивчення та узагальнення положень вище наведеного НПА надає можливість сформувати *мету та послідовність* проведення державної експертизи у сфері КЗІ. [61, 63]

Державна експертиза у сфері криптографічного захисту інформації проводиться *з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їхньої відповідності вимогам нормативних документів з криптографічного захисту інформації та можливості їх використання за призначенням для забезпечення КЗІ.*

Об'єктами експертизи є:

засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ;

звіти про наукові дослідження і розробки, результати тематичних досліджень, інші результати наукової та науково-технічної діяльності у сфері КЗІ;

криптографічні алгоритми та протоколи;

алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключових даних;

криптографічні системи, засоби та обладнання КЗІ (далі – криптографічні засоби);

положення державних і міждержавних програм та проєктів державного значення в частині, що стосується КЗІ.

Експертиза є обов'язковою або добровільною.

Обов'язковій експертизі підлягають:

засоби та методи, призначені для розробки, дослідження, виробництва та випробувань засобів криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом;

криптографічні алгоритми та криптографічні протоколи, які планується визначити як такі, що рекомендовані для використання або як національні стандарти;

алгоритми, протоколи, засоби та системи генерації, тестування та розподілу ключів;

криптосистеми, засоби й обладнання криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом;

засоби категорії «П», що використовуються як засоби кваліфікованого електронного підпису чи печатки;

засоби, що реалізують криптоперетворення та/або механізми імітозахисту та використовуються в системах зв’язку, управління та озброєння;

засоби обробки та передачі державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, які реалізують функції криптографічного захисту інформації;

криптосистеми, засоби та обладнання КЗІ іноземного виробництва, які підлягають експортному контролю;

результати тематичних досліджень.

Суб'єктами експертизи є:

Замовники експертизи;

Адміністрація Держспецзв'язку;

Експертні заклади;

Спеціалізовані організації.

Замовники експертизи ініціюють експертизу відповідних об’єктів.

Організацію експертизи здійснює безкоштовно Адміністрація Держспецзв'язку. Для координації та здійснення експертизи в Адміністрації Держспецзв'язку *створюється Експертна комісія з питань проведення державної експертизи в сфері криптографічного захисту інформації Держспецзв'язку (далі – Експертна комісія)*. Експертна комісія підпорядковується Голові Держспецзв'язку. Результати експертних

(тематичних) досліджень розглядає Експертна комісія, за результатами чого Адміністрація Держспецзв'язку видає *експертний висновок.*

Експертні (тематичні) дослідження проводять Експертні заклади, Спеціалізовані організації або Адміністрація Держспецзв'язку за договорами на проведення експертних (тематичних) досліджень.

Порядок організації та проведення експертизи полягає у наступному.

1. Для проведення експертизи таких об'єктів, як:

засоби, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ,

засоби та системи генерації, тестування і розподілу ключових даних;

криптографічні системи, засоби та обладнання КЗІ

Замовник подає до Адміністрації Держспецзв'язку заявку на проведення державної експертизи в сфері криптографічного захисту інформації (додаток 1). До заявки на експертизу перелічених вище об'єктів (далі – криптографічні засоби) додається комплект документів та матеріалів згідно з переліком документів та матеріалів, необхідних для проведення експертизи криптографічних засобів вітчизняного виробництва (додаток 2), або переліком документів та матеріалів, необхідних для проведення експертизи криптографічних засобів іноземного виробництва (додаток 3).

З урахуванням особливостей криптографічних засобів зазначені вище переліки можуть уточнюватися.

У складі комплекту документів на проведення державної експертизи криптографічних засобів вітчизняного виробництва, які виготовляються серійно, обов'язково подаються технічні умови (проєкт технічних умов), затверджені та зареєстровані в установленому порядку.

2. Для проведення експертизи таких об'єктів, як:

методи, призначені для розробки, дослідження, виробництва та випробувань засобів КЗІ;

звіти про наукові дослідження і розробки, результати тематичних досліджень, інші результати наукової та науково-технічної діяльності у сфері КЗІ;

криптографічні алгоритми та протоколи, методи генерації, тестування та розподілу ключових даних;

положення державних і міждержавних програм та проєктів державного значення в частині, що стосується КЗІ

Замовник експертизи подає до Адміністрації Держспецзв'язку заявку на проведення експертизи, відповідний об'єкт експертизи, а також документи та матеріали з обґрунтуванням змісту об'єкта експертизи.

Документи та матеріали на об'єкт експертизи надаються українською мовою.

3. *Адміністрація Держспецзв'язку в місячний термін* з дня отримання заявки розглядає її та *здійснює аналіз наданих документів і матеріалів*.

Під час аналізу наданих документів та матеріалів перевіряються:

наявність та достатність документів, матеріалів, зразків для проведення експертизи;

наявність документів, що підтверджують походження об'єкта експертизи, розміри партії криптографічних засобів;

перелік документів, матеріалів, спеціального устаткування для проведення експертних досліджень;

можливість ідентифікації криптографічних засобів;

достовірність, правильність оформлення та термін дії наданої замовником документації;

можливість експертних закладів проводити відповідні експертні дослідження.

4. У разі визначення в заявці Експертного закладу, що планується до проведення експертних *досліджень вперше, до неї додатково додаються*:

перелік фахівців, що мають проводити експертні дослідження, із зазначенням рівня їхньої освіти (який вищий навчальний заклад та в якому році закінчив, яка присвоєна кваліфікація, отримана спеціальність) і досвіду з розробки або досліджень у сфері криптографічного захисту інформації;

перелік матеріальних засобів (із зазначенням їх технічних характеристик), що призначені для проведення досліджень.

Адміністрація Держспецзв'язку може обґрунтовано визначити необхідність надання замовником додаткових документів, матеріалів, спеціального устаткування з урахуванням особливостей об'єкта експертизи, зокрема особливостей реалізації криптографічного засобу, порядку та схеми проведення експертизи, мети проведення експертизи, можливості (необхідності) виходу з ладу або руйнації зразків криптографічного засобу, його габаритних показників тощо.

5. *У разі відповідності заявки встановленим вимогам Адміністрація Держспецзв'язку готує рішення Адміністрації Держспецзв'язку* за заявкою на проведення державної експертизи в сфері криптографічного захисту інформації (додаток 4) (далі – рішення Адміністрації Держспецзв'язку), у якому визначаються *умови проведення експертизи, перелік додаткових*

документів та матеріалів, необхідних для проведення експертизи, схема проведення експертизи за варіантами схем проведення експертизи криптографічних засобів (додаток 5), а також Експертний заклад.

Експертний заклад призначається Адміністрацією Держспецзв'язку з урахуванням пропозицій замовника.

6. Про рішення Адміністрації Держспецзв'язку *Замовнику експертизи та Експертному закладу протягом десяти днів після його ухвалення надсилається письмове повідомлення*.

7. *Договір на проведення експертних (тематичних) досліджень між Замовником та Експертним закладом* (Спеціалізованою організацією) укладається після отримання ними повідомлення про рішення Адміністрації Держспецзв'язку.

Про укладення договору та передбачений договором термін завершення експертних (тематичних) досліджень *Замовник експертизи письмово інформує Адміністрацію Держспецзв'язку.*

8. *Процедури відбору та ідентифікації зразків криптографічних засобів,* що надаються на експертизу, проводяться після ухвалення рішення Адміністрації Держспецзв'язку, а у разі укладення договору – після його підписання.

Ідентифікація та відбір зразків об'єкта експертизи проводять представники Адміністрації Держспецзв'язку у присутності представників Замовника та визначеного у рішенні Адміністрації Держспецзв'язку Експертного закладу. Ідентифікація зразків оформлюється актом ідентифікації зразків для проведення державної експертизи у сфері криптографічного захисту інформації (додаток 6).

Відбір зразків програмного забезпечення (його складових частин) засобу оформлюється актом відбору зразків для проведення державної експертизи у сфері криптографічного захисту інформації (додаток 7).

9. Державна експертиза відібраних зразків здійснюється шляхом експертних досліджень.

Для проведення експертних досліджень *експертними закладами у місячний термін з моменту укладання договору* на проведення досліджень та отримання об'єкта експертизи і необхідного комплекту документів *розробляються програми та методики проведення експертних досліджень*. Під час підготовки програм та методик експертні заклади можуть уточнити перелік необхідних для проведення досліджень документів, матеріалів та спеціального устаткування. Зазначений перелік погоджується з Адміністрацією Держспецзв'язку.

За результатами розгляду *Експертною комісією програми затверджуються, а методики погоджуються керівником структурного підрозділу Адміністрації Держспецзв'язку, який організовує експертизу*, або особою, яка виконує його обов'язки.

10. За результатами експертних досліджень *Експертні заклади готують, затверджують та подають до Адміністрації Держспецзв'язку протоколи експертних досліджень. Зміст протоколів експертних досліджень повинен відповідати вимогам програми та методики проведення експертних досліджень.*

11. *Підрозділ Адміністрації Держспецзв'язку, який організовує експертизу, протягом місяця з дня отримання протоколів* експертних досліджень розглядає їх на предмет відповідності програмі та методиці проведення експертних досліджень, повноти, об'єктивності, достатності та інших характеристик, *готує пропозиції та вносить їх на засідання Експертної комісії.*

12. *У разі відповідності протоколів* експертних досліджень програмі та методиці проведення експертних досліджень *на підставі рішення Експертної комісії Адміністрація Держспецзв'язку готує та надсилає Замовнику експертний висновок (додаток 8)*. Термін підготовки та надсилання замовнику експертного висновку не повинен перевищувати 20 робочих днів з дати ухвалення рішення Експертною комісією.

Після закінчення експертизи всі матеріальні цінності, у тому числі зразки-свідки, в обов'язковому порядку повертаються замовнику, який повинен забезпечити зберігання зразка-свідка протягом терміну дії експертного висновку в стані, що дає змогу його використання для верифікації.

13. *Адміністрація Держспецзв'язку здійснює контроль за проведенням експертних досліджень, а також за виробництвом криптографічних засобів*.

Термін дії експертного висновку визначається з урахуванням криптографічних якостей криптографічного засобу, терміну дії нормативних документів, умов та граничного терміну експлуатації криптографічного засобу, але не більше термінів, зазначених у додатку 5 до Положення.

Експертний висновок може бути виданий на один зразок криптографічного засобу, партію засобів, а також засіб, що виробляється серійно, за наявності технічних умов на нього.

Експертні висновки, термін дії яких закінчився, утрачають чинність.

Експертний висновок може бути анульований за пропозицією Експертної комісії за наявності підстав, передбачених п. 2.3.21 Положення.

Оскарження результатів експертизи здійснюється відповідно до вимог законодавства України.

Проведення державної експертизи пов’язано із документуванням усіх робіт, які передбачені вимогами вище наведеного Положення, відпрацювання цілої низки обов’язкових документів. У наступному питанні наведемо перелік найголовніших із них.

3.4.3 Документи, що розробляються під час проведення експертизи вітчизняних та іноземних засобів КЗІ

Перелік документів, що розробляються під час проведення експертизи вітчизняних та іноземних засобів КЗІ, формується на підставі розглянутого вище навчального матеріалу під керівництвом викладача за активної участі здобувачів вищої освіти.

Проведення державної експертизи засобів КЗІ пов’язано із відпрацюванням цілої низки документів як Замовником експертизи, так і іншими суб’єктами експертизи.

Проаналізуємо вимоги НПА та сформуємо перелік основних документів, які відпрацьовуються суб’єктами державної експертизи в процесі її проведення. [61, 63]

Замовником державної експертизи *відпрацьовуються та за встановленим порядком подаються*:

заявка на проведення державної експертизи в сфері криптографічного захисту інформації (додаток 1 до Положення) (до якої *додається комплект документів та матеріалів згідно з переліком документів та матеріалів,* необхідних для проведення експертизи криптографічних засобів вітчизняного виробництва (додаток 2) або *переліком документів та матеріалів, необхідних для проведення експертизи криптографічних засобів іноземного виробництва* (додаток 3), а також *технічні умови (проєкт технічних умов) на зразок КЗІ*, затверджені та зареєстровані в установленому порядку)

або

заявка на проведення державної експертизи в сфері криптографічного захисту інформації (додаток 1 до Положення), відповідний об'єкт експертизи, а також документи та матеріали з обґрунтуванням змісту об'єкта експертизи.

(*У разі визначення в заявці Експертного закладу, що планується до проведення експертних досліджень вперше, до неї додатково додаються:

перелік фахівців, що мають проводити експертні дослідження, із зазначенням рівня їхньої освіти (який вищий навчальний заклад та в якому році закінчив, яка присвоєна кваліфікація, отримана спеціальність) і досвіду з розробки або досліджень у сфері криптографічного захисту інформації;

перелік матеріальних засобів (із зазначенням їхніх технічних характеристик), що призначені для проведення досліджень);

договір на проведення експертних (тематичних) досліджень (разом *із Експертним закладом* (Спеціалізованою організацією);

лист-повідомлення щодо укладання договору на проведення експертних (тематичних) досліджень на адресу Адміністрації Держспецзв'язку.

***Адміністрація Держспецзв'язку (організатор) державної експертизи відпрацьовує**:*

рішення Адміністрації Держспецзв'язку на проведення державної експертизи в сфері криптографічного захисту інформації (додаток 4) за заявкою Замовника;

схема проведення експертизи криптографічних засобів (додаток 5);

листи-повідомлення щодо рішення Адміністрації Держспецзв'язку на проведення державної експертизи в сфері криптографічного захисту інформації на адресу Замовника експертизи та Експертного закладу;

акт ідентифікації зразків для проведення державної експертизи у сфері криптографічного захисту інформації (додаток 6) або акт відбору зразків для проведення державної експертизи у сфері криптографічного захисту інформації (додаток 7):

пропозиції для ухвалення на Експертній комісії за результатами аналізу протоколів експертних досліджень наданих на експертизу зразків КЗІ;

рішення Експертної комісії Адміністрації Держспецзв'язку;

експертний висновок (додаток 8);

рішення Експертної комісії Адміністрації Держспецзв'язку про анулювання експертного висновку (за наявності відповідних підстав).

Експертний заклад (Спеціалізована організація) відпрацьовує:

договір на проведення експертних (тематичних) досліджень (разом із Замовником експертизи);

погоджені з Адміністрацією Держспецзв'язку *програми та методики проведення експертних досліджень* (за необхідності додатково – перелік

необхідних для проведення досліджень документів, матеріалів та спеціального устаткування);

протоколи експертних досліджень наданих на експертизу зразків КЗІ.

Отже, *державна експертиза у сфері КЗІ є важливим процесом дослідження, перевірки, аналізу та оцінки об'єкта експертизи щодо його відповідності вимогам нормативних документів з криптографічного захисту інформації та можливості використання за призначенням для забезпечення КЗІ із обов'язковим юридичним оформленням кожного етапу експертизи.*

Висновки до розділу 3

У розділі 3 розглянуто напрямки нормативно-правового забезпечення в сфері криптографічного захисту інформації, ієрархію законодавчих та нормативно-правових актів держави в цьому секторі ІБ, їхнє призначення, побудову та основні положення.

У розглянутій ієрархії НПА "Положення про порядок здійснення криптографічного захисту інформації в Україні" (указ Президента України від 22 травня 1998 року № 505/98) займає одне з центральних місць. Короткий за обсягом, але дуже інформативний за змістом, цей НПА накреслює напрямки нормативно-правового забезпечення в даному секторі ІБ. Із його положень стає зрозумілим, що кожен напрямок діяльності в сфері криптографічного захисту інформації, а саме: розробка, виготовлення, ввезення, вивезення, реалізація, використання, утилізація засобів криптографічного захисту інформації, надання будь-яких послуг із криптографічного захисту інформації тощо, повинні бути чітко регламентовані вимогами відповідних правил, інструкцій, положень, настанов. Такі нормативні документи повинні пройти обов'язкову процедуру погодження з Держспецзв'язком України.

Важливе місце у ієрархії відведено також й "Положенню про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації" (наказ Адміністрації Держспецзв'язку від 20 липня 2007 року за № 141). Вимогами цього НПА регламентовано загальний порядок виконання обов'язкових заходів на етапах розроблення, виробництва, експлуатації, утилізації засобів КЗІ. Різноманіття видів засобів криптографічного захисту інформації, особливості їхнього призначення та побудови повинні враховуватися під час усіх етапів їхнього життєвого циклу. Така жорстка регламентація поводження із засобами КЗІ обґрунтовує необхідність ліцензування діяльності відповідних установ, діяльність яких пов'язана із будь-яким етапом їх життєвого циклу.

Ліцензування діяльності суб'єктів, зайнятих у сфері криптографічного захисту інформації, встановлено вимогами Закону України “Про ліцензування видів господарської діяльності” від 2 березня 2015 року № 222-VIII, а також постановою КМУ від 16 листопада 2016 року № 821 “Про деякі питання ліцензування господарської діяльності у галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України”. Положеннями НПА для таких суб'єктів господарської діяльності встановлюються певні ліцензійні умови.

Ці ліцензійні умови є конкретними, багатоплановими та досить жорсткими вимогами щодо умов, дотримуючись яких суб'єкти можуть здійснювати діяльність в галузі КЗІ. Процес отримання суб’єктами ліцензії на право займатись відповідною господарською діяльністю не є простою справою. Він потребує від суб’єктів точного та повного виконання всіх положень ліцензійних вимог, як на етапі отримання ліцензії, так і під час спрямування усіх технологічних процесів господарської діяльності в русло обов’язкового дотримання вимог чинних НПА в цій сфері протягом усього терміну дії ліцензії. За невиконання ліцензійних умов суб’єкти господарської діяльності можуть бути позбавлені ліцензії.

Перелік законодавчих та нормативно-правових актів, які визначають обов’язковість застосування криптографічного захисту інформації, яка є власністю держави, розпочинає Закон України “Про електронні документи та електронний документообіг” від 22 травня 2003 року № 851-IV. Він встановлює основні організаційно-правові засади електронного документообігу та закладає законодавчі основи створення нормативно-правового забезпечення у вигляді цілої низки НПА, які деталізують порядок реалізації обов’язкових процесів документообігу із забезпеченням технологій криптографічного захисту інформації на кожному із них.

Положення цього Закону передбачають дотримання порядку формування документів, організації та здійснення документообігу в установах, встановленого відповідними державними стандартами та інструкціями з документоведення. Вимоги стандартів та інструкцій повинні виконуватись незалежно від того, в якому вигляді (паперовому або електронному) створені документи.

Такими НПА в державі є ДСТУ 4163:2020 “Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів”, “Типова інструкція з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади” (затверджена постановою Кабінету Міністрів України від 17 січня 2018 року № 55). Ці НПА є базовими, вони встановлюють вимоги щодо документування управлінської інформації та організації роботи з документами, створеними у паперовій формі. Вимоги цих НПА, а

також положення галузевої “Інструкції з організації діловодства в Державній службі спеціального зв’язку та захисту інформації України”, введеної в дію наказом Адміністрації Держспецзв’язку України від 29 лютого 2012 року № 100, є обов’язковими в установах ДССЗЗІ України.

Враховуючи вимоги НПА, які наведено вище, наступні НПА “Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198) та “Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну (постанова КМУ від 17 січня 2018 року № 55) встановлюють вимоги щодо впровадження електронного документообігу та організації роботи з електронними документами у діловодствах установ держави.

Виконання цих вимог забезпечує безпеку відкритої інформації, що є власністю держави, в електронній формі і є обов’язковими для державних органів, органів місцевого самоврядування, підприємств, установ та організацій незалежно від форм власності.

Вимоги щодо обов’язковості застосування криптографічного захисту інформації мають пролонгацію й у секторі надання електронних довірчих послуг суб’єктам інформаційної діяльності. Ці вимоги підтверджені у положеннях Закону України “Про електронну ідентифікацію та електронні довірчі послуги” від 05 жовтня 2017 року № 2155-VIII (зі змінами) та “Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності”, введеного в дію постановою КМУ від 01 серпня 2023 року № 798.

Ці важливі складові нормативно-правового забезпечення інформаційної безпеки визначають правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов’язки суб’єктів правових відносин у сфері електронних довірчих послуг (зокрема й ДССЗЗІ України), порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також із врахуванням положень НПА держав Євросоюзу конкретизують вимоги щодо порядку використання кваліфікованих електронних довірчих послуг в державних установах.

Важливість забезпечення цілісності інформаційних ресурсів для суб’єктів інформаційних відносин обґрунтовує підвищені вимоги щодо надійності криптографічного захисту інформації, які реалізовані в технологіях електронного документообігу, а також наданні кваліфікованих електронних довірчих послуг. Надійність криптографічного захисту

інформації може бути гарантована тільки за умови проходження цими технологіями та відповідними засобами КЗІ державної експертизи.

Вимогами "Положення про державну експертизу у сфері криптографічного захисту інформації", введеного в дію наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрованого в Міністерстві юстиції України 16 липня 2008 року за № 651/15342, в редакції 2020 року установлено порядок організації та проведення державної експертизи у сфері криптографічного захисту інформації в Україні.

Державна експертиза у цій сфері є важливим процесом дослідження, перевірки, аналізу та оцінки об'єкту експертизи щодо його відповідності вимогам нормативних документів з криптографічного захисту інформації та можливості використання за призначенням із обов'язковим документуванням кожного етапу експертизи. Тільки за умов успішного проходження державної експертизи об'єкти експертизи можуть бути застосовані установами держави.

Отже, за результатами розгляду та аналізу положень наведених основних нормативно-правових актів України з криптографічного захисту інформації, можна зробити висновки щодо великого обсягу, багатовекторності, складності та жорсткої регламентації робіт у сфері КЗІ. Ці висновки обґрунтовують необхідність системного та поглибленого вивчення вимог законодавчих, нормативно-правових актів та нормативних документів, чинних у сфері КЗІ, як теоретичного підґрунтя у формуванні необхідних професійних компетентностей майбутніх фахівців ДССЗЗІ.

ЗАПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ (ПРОВЕДЕННЯ ПОТОЧНОГО КОНТРОЛЮ)

1. Доповісти про призначення та спрямованість змісту "Положення про порядок здійснення криптографічного захисту інформації в Україні" (указ Президента України від 22 травня1998 року № 505/98).

2. Відповідно до змісту "Положення про порядок здійснення криптографічного захисту інформації в Україні", введеного в дію указом Президента України від 22 травня 1998 року № 505/98 надати визначення термінам: *"засіб криптографічного захисту інформації", "криптографічна система (криптосистема)", "система криптографічного захисту інформації"*.

3. Доповісти про головні вимоги до криптосистем і засобів криптографічного захисту, які створюються для захисту інформації, що становить державну таємницю, та службової інформації, що є власністю держави?

4. Доповісти про призначення та спрямованість вимог “Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації” (наказ Адміністрації Держспецзв’язку від 20 липня 2007 року за № 141).

5. Відповідно до вимог “Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації”, введеного у дію наказом Адміністрації Держспецзв’язку від 20 липня 2007 року за № 14 доповісти:

на які види поділяються засоби КЗІ в залежності від їх виконання?

на які категорії поділяються засоби КЗІ в залежності від їх призначення?

на які класи поділяються засоби КЗІ з урахуванням установленого рівня можливостей потенційного порушника?

6. На який термін видається ліцензія суб’єктам ліцензування на провадження ними визначеного виду господарської діяльності у сфері ТЗІ та КЗІ (відповідно до вимог Закону України “Про ліцензування видів господарської діяльності” від 02 березня 2015 року № 222-VIII та постанови Кабінету Міністрів України від 16 листопада 2016 року № 821)?

7. Доповісти про призначення та спрямованість змісту:

Закону України “Про електронні документи та електронний документообіг” від 22 травня 2003 року № 851- IV;

ДСТУ 4163:2020 “Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання документів”;

“Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198);

“Типової інструкції з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну” (постанова КМУ від 17 січня 2018 року № 55).

8. Як має бути оформлений електронний документ (відповідно до положень НПА “Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання” (наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 за № 1421/26198))?

9. Доповісти про призначення та спрямованість змісту:

Закону України “Про електронну ідентифікацію та електронні довірчі послуги” від 05 жовтня 2017 року № 2155-VIII, (зі змінами);

НПА “Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах,

установах та організаціями державної форми власності" (постанова КМУ від 01 серпня 2023 року № 798);

10. Відповідно до положень наведених вище законодавчих та нормативно-правових документів надати визначення термінам: *"електронний документ", "обов'язковий реквізит електронного документа", "електронний цифровий підпис", "електронна довірча послуга"*.

11. Хто є суб'єктами відносин у сфері електронних довірчих послуг (надати відповідь відповідно до положень Закону України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155- VIII, зі змінами)?

12. Якими шляхами можуть здійснюватися заходи державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг Адміністрацією Держспецзв'язку (надати відповідь відповідно до положень Закону України "Про електронну ідентифікацію та електронні довірчі послуги" від 05 жовтня 2017 року № 2155- VIII, зі змінами)?

13. Доповісти про перелік об'єктів та суб'єктів експертизи відповідно до положень НПА "Положення про державну експертизу у сфері криптографічного захисту інформації", введеного в дію наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрованого в Міністерстві юстиції України 16 липня 2008 року за № 651/15342, в редакції 2020 року.

14. Доповісти про порядок проведення державної експертизи у сфері КЗІ відповідно до положень НПА "Положення про державну експертизу у сфері криптографічного захисту інформації", введеного в дію наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрованого в Міністерстві юстиції України 16 липня 2008 року за № 651/15342, в редакції 2020 року.

15. Доповісти про підстави анулювання раніше виданого експертного висновку на засоби КЗІ (відповідно до положень НПА "Положення про державну експертизу у сфері криптографічного захисту інформації", введеного в дію наказом Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрованого в Міністерстві юстиції України 16 липня 2008 року за № 651/15342, в редакції 2020 року).

16. Який орган створений в Адміністрації Держспецзв'язку з метою організації та проведення експертиз (відповідно до "Положення про державну експертизу у сфері криптографічного захисту інформації" (наказ Адміністрації Держспецзв'язку від 23 червня 2008 року № 100, зареєстрований в Міністерстві юстиції України 16 липня 2008 року за № 651/15342))?

ВИСНОВОК

У навчальному посібнику систематизовано викладений матеріал з нормативно-правового забезпечення інформаційної безпеки держави, а також методичні рекомендації щодо організації та проведення занять відповідного освітнього компоненту досягли головної мети, а саме: у певній методичній послідовності на тлі сучасних проблем та викликів у сфері інформаційної безпеки держави викладено та проаналізовано чинну систему нормативно-правового забезпечення України у сфері інформаційної безпеки; увага здобувачів вищої освіти зосереджена на структурі та положеннях основних законодавчих та нормативно-правових актів України щодо забезпечення захисту інформаційних ресурсів держави у різних секторах ІБ; зроблено акцент на нормативно-правовому забезпеченні тих секторів ІБ, в яких для Державної служби спеціального зв'язку та захисту інформації України визначені певні повноваження та завдання; надана методична допомога здобувачам вищої освіти у формуванні відповідних компетентностей, що дозволять їм після завершення навчання успішно виконувати функціональні обов'язки у межах займаних посад, на які будуть призначені.

Перелік завдань ДССЗЗІ України є дуже широким. Як відомо із матеріалу, розглянутого у пункті *1.6. Класифікація та повноваження суб'єктів забезпечення ІБ України* Розділу 1 цього посібника, відповідно до положень Закону України "Про державну службу спеціального зв'язку та захисту інформації" від 23 лютого 2006 року № 3475-IV (зі змінами) ***кількість завдань, покладених на службу, дорівнює 94***. Ці завдання є різноплановими та стосуються різних секторів ІБ держави. За такої їхньої кількості та різноплановості було дуже важливо зробити акценти на нормативно-правовому забезпеченні тих секторів ІБ, до яких здобувачі вищої освіти можуть мати безпосередній стосунок після закінчення навчання та призначення на первинні посади в установи ДССЗЗІ України.

Саме такий підхід до викладання змісту кожного із розділів був пріоритетним для укладачів посібника. Він сприятиме послідовному формуванню у здобувачів, починаючи з другого року їхнього навчання в інституті, необхідних важливих фахових компетентностей, передбачених стандартом вищої освіти України зі спеціальності *F5 (125) Кібербезпека та захист інформації* галузі знань 12 "Інформаційні технології" для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04 жовтня 2018 року № 1074 (зі змінами 2024 року), а також положеннями відповідної освітньо-професійної програми підготовки бакалаврів "Безпека державних інформаційних ресурсів".

Побудова та зміст розділів навчального посібника сприяє успішному вирішенню й іншого завдання, що стояло перед його укладачами, а саме:

наданні методичної допомоги викладачам інституту, задіяним у викладанні матеріалу освітнього компоненту “Нормативно-правове забезпечення інформаційної безпеки” щодо системного відпрацювання необхідних навчально-методичних матеріалів, якісної підготовки та проведення навчальних занять.

Навчальний посібник може бути рекомендований для здобувачів вищої освіти ступеня бакалавр, які навчаються в Інституті спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського” та після завершення навчання плануються для розміщення на посади у відповідні установи Державної служби спеціального зв’язку та захисту інформації України, а також науково-педагогічним працівникам Інституту.

Отже, поставлені у навчальному посібнику завдання виконано та мета досягнута.

СПИСОК ВИКОРИСТАНИХ ТА РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Стандарт вищої освіти України зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти, затверджений наказом Міністерства освіти та науки України від 04.10.2018 № 1074 (у редакції наказу Міністерства освіти і науки України від 29.10.2024 № 1547) [Електронний ресурс] – Режим доступу: https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf.
2. Безпека державних інформаційних ресурсів. Освітньо-професійна програма зі спеціальності 125 *Кібербезпека та захист інформації*, кваліфікації *бакалавр з кібербезпеки та захисту інформації*, затверджена Вченою радою КПІ ім. Ігоря Сікорського від 20 січня 2025 року, протокол № 1 [Електронний ресурс] – Режим доступу: https://osvita.kpi.ua/sites/default/files/opfiles/125_oppb_bdir_2024o.pdf.
3. Робоча програма освітнього компонента (силабус) Нормативно-правове забезпечення інформаційної безпеки, ухвалена Методичною комісією ІСЗЗІ КПІ ім. Ігоря Сікорського, протокол від 27.06.2024 № 6.
4. Звіт про науково-дослідну роботу формування антитерористичної компетентності у фахівців національної системи кібербезпеки / наук. кер. С. С. Кудінов. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. – 109 с.
5. Теоретико-правові засади формування антитерористичної компетентності у фахівців національної системи кібербезпеки України: монографія. / Кудінов С.С., Пучков О.О. та інші. – Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2024. – 260 с.
6. Інформаційна безпека: підруч. для студ. ВНЗ / В. Остроухов, М. Присяжнюк, О. Формагей, М. Чеховська, рук. В. Остроухов. – К.: Ліра-К, 2021. – 412 с.
7. Інформаційна безпека держави: підруч. для студ. ВНЗ / В. Петрик, М. Присяжнюк, Д. Мельник. – в 2 Т. – Т.1. – Київ: ІСЗЗІ НТУУ КПІ, 2016. – 264 с.
8. Конституція України (Основний закон), (зі змінами) : офіц. текст. – Київ : Відомості Верховної Ради України (ВВР), 1996. – 87 с.
9. Стратегія національної безпеки України [Електронний ресурс] : указ Президента України від 14 вересня 2020 року № 392/2020 : станом на 16 лютого 2022 р. – Режим доступу: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 10.04.2025). – Назва з екрана.
10. Стратегія інформаційної безпеки [Електронний ресурс] : Указ Президента України від 28 грудня 2021 р. № 685/2021 : станом на 30 грудня 2021 р. –

Режим доступу: https://zakon.rada.gov.ua/laws/show/n0080525-21 (дата звернення: 10.04.2025). – Назва з екрана.

11. Про національну безпеку України [Електронний ресурс] : Закон України від 21 червня 2018 року № 2469-VIII : станом на 27 березня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/ (дата звернення: 27.03.2025). – Назва з екрана.
12. Про інформацію [Електронний ресурс] : Закон України від 02 жовтня 1992 року № 2657- XII : станом на 10 жовтня 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 27.03.2025). – Назва з екрана.
13. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс] : Закон України від 05 липня 1994 року № 2657-XII : станом на 27 березня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 10.04.2025). – Назва з екрана.
14. Про електронні комунікації [Електронний ресурс] : Закон України від 16 грудня 2020 року № 1089-IX : станом на 17 грудня 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 10.04.2025). – Назва з екрана.
15. Про електронні документи та електронний документообіг [Електронний ресурс] : Закон України від 22 травня 2003 року № 851-IV : станом на 01 грудня 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 10.04.2025). – Назва з екрана.
16. Про захист персональних даних [Електронний ресурс] : Закон України від 01 червня 2010 року № 2297-VI : станом на 19 грудня 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.04.2025). – Назва з екрана.
17. Про Національну систему конфіденційного зв'язку [Електронний ресурс] : Закон України від 10 січня 2002 року № 2919-III : станом на 03 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2919-14#Text (дата звернення: 10.04.2025). – Назва з екрана.
18. Про державну таємницю [Електронний ресурс] : Закон України від 21 січня 1994 року № 3856-XII: станом на 30 жовтня 2024 р.– Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 10.04.2025). – Назва з екрана.
19. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 05 жовтня 2017 року № 2163-VIII : станом на 20 квітня 2025 р.– Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.04.2025). – Назва з екрана.
20. Стратегія кібербезпеки України [Електронний ресурс] : Указ Президента України від 26 серпня 2021 року № 447/2021 : станом на 26 серпня 2021 р. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.04.2025). – Назва з екрана.
21. Про критичну інфраструктуру [Електронний ресурс] : Закон України від 16 листопада 2021 року № 1882-IX: станом на 21 вересня 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 23.04.2025). – Назва з екрана.
22. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [Електронний ресурс] : Постанова КМУ від 19 червня 2019 року № 518 : станом на 07 вересня 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 23.04.2025). – Назва з екрана.
23. ДСТУ ISO IEC 27001:2015. Інформаційні технології. Методи забезпечення безпеки. Системи менеджмента інформаційної безпеки. Вимоги. – [Чинний від 2017-01-01]. – Київ : УкрНДНЦ, 2016. – 22 с.
24. ДСТУ ISO IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. – [Чинний від 2017-12-18]. – Київ : УкрНДНЦ, 2016. – 66 с.
25. ДСТУ ISO IEC 9798-1:2002. Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 1. Загальні положення. – [Чинний від 2005-09-27]. – Київ : Держспоживстандарт України, 2005. – 10 с.
26. ДСТУ ISO IEC 9798-3:2002. Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використання методу цифрового підпису. – [Чинний від 2005-09-27]. – Київ : Держспоживстандарт України, 2005. – 8 с.
27. Про державну службу спеціального зв'язку та захисту інформації [Електронний ресурс] : Закон України від 23 лютого 2006 року № 1882-IX: станом на 20 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 23.04.2025). – Назва з екрана.
28. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс] : Постанова КМУ від 3 вересня 2014 року № 411: станом на 07 вересня 2022 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text (дата звернення: 21.11.2024). – Назва з екрана.
29. Кримінальний процесуальний кодекс України [Електронний ресурс] : Закон України від 13 квітня 2006 року № 4651-VI: станом на 26 лютого 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 23.04.2025). – Назва з екрана.
30. Кодекс України про адміністративні правопорушення [Електронний ресурс] : Постанова Верховної Ради Української РСР від 07 грудня 1984 року № 8074-10: станом на 17 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 23.04.2025). – Назва з екрана.

31. ДСТУ 2226:1993. Автоматизовані системи. Терміни та визначення : [Чинний з 1993-09-09]. – Київ : Держспоживстандарт України, 1993. – 90 с.
32. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : Постанова КМУ від 29 березня 2006 року № 373 : станом на 18 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 23.04.2025). – Назва з екрана.
33. НД ТЗІ 3.6-004-2021. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці [Електронний ресурс] : Проєкт до затвердження наказом Адміністрації Держспецзв'язку України. – Режим доступу: https://cip.gov.ua › api › attachment › download (дата звернення: 23.04.2025). – Назва з екрана.
34. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. – Режим доступу: https://tzi.com.ua/downloads/2.5-005%20-99.pdf (дата звернення: 23.04.2025). – Назва з екрана.
35. НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 13 грудня 2002 року № 84 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28 грудня 2012 року № 806. – Режим доступу: https://tzi.com.ua/downloads/2.5-008-2002.pdf (дата звернення: 23.04.2025). – Назва з екрана.
36. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 28 квітня 1999 року № 22 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28 грудня 2012 року № 806. – Режим доступу: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 23.04.2025). – Назва з екрана.
37. Звід відомостей, що становлять державну таємницю [Електронний ресурс] : Наказ Центрального управління Служби безпеки України від 23 грудня 2020 року № 383, зареєстровано в Міністерстві юстиції України 14 січня 2021 року за № 52/35674: станом на 09 травня 2025 р. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/z0052-21#Text (дата звернення: 13.05.2025). – Назва з екрана.
38. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах [Електронний ресурс] : Постанова КМУ від 16 лютого 1998 року № 180: станом на 16 серпня 2010 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/180-98-п#Text (дата звернення: 23.04.2025). – Назва з екрана.
39. ДСТУ 3396.0:1996 Захист інформації. Технічний захист інформації. Основні положення : [Чинний з 1997-01-01]. – Київ : Держспоживстандарт України, 1996. – 8 с.
40. ДСТУ 3396.1:1996 Захист інформації. Технічний захист інформації. Порядок проведення робіт : [Чинний з 1997-07-01]. – Київ : Держспоживстандарт України, 1996. – 6 с .
41. НД ТЗІ 3.7-003-2023. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі [Електронний ресурс] : Наказ Адміністрації Держспецзв’язку України від 28 жовтня 2023 року № 924. – Режим доступу: https://tzi.com.ua/downloads/2.5-005%20-99.pdf (дата звернення: 23.04.2025). – Назва з екрана.
42. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 року № 22 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. – Режим доступу: https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення: 23.04.2025). – Назва з екрана.
43. Концепція технічного захисту інформації в Україні [Електронний ресурс] : Постанова КМУ від 08 жовтня 1997 року № 1126 : станом на 13 жовтня 2011 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1126-97-п#Text (дата звернення: 23.04.2025). – Назва з екрана.
44. Положення про технічний захист інформації в Україні [Електронний ресурс] : Указ Президента України від 27 вересня 1999 року № 1229/99: станом на 04 травня 2008 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 10.04.2025). – Назва з екрана.
45. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 року № 53 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28 грудня 2012 року № 806. – Режим

доступу: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 23.04.2025). – Назва з екрана.

46. НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем [Електронний ресурс] : Проєкт до затвердження наказом Адміністрації Держспецзв'язку України. – Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення: 23.04.2025). – Назва з екрана.
47. Порядок здійснення державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 16 травня 2007 року № 87 зі змінами згідно наказу Адміністрації Держспецзв'язку від 08 квітня 2021 року № 61. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0785-07#Text (дата звернення: 23.04.2025). – Назва з екрана.
48. Положення про державну експертизу в сфері технічного захисту інформації [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 16 травня 2007 року № 93, зареєстровано в Міністерстві юстиції України 16 липня 2007 року за № 820/14087. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07#Text (дата звернення: 23.04.2025). – Назва з екрана.
49. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 25 березня 2011 року № 65 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. – Режим доступу: https://tzi.com.ua/downloads/2.6-001-11.pdf (дата звернення: 23.04.2025). – Назва з екрана.
50. Положення про порядок здійснення криптографічного захисту інформації в Україні [Електронний ресурс] : Указ Президента України від 22 травня 1998 року № 505/98 зі змінами від 28 серпня 2009 року № 693/2009 : станом на 12 вересня 2009 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/505/98#Text (дата звернення: 10.04.2025). – Назва з екрана.
51. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 20 липня 2007 року за № 141 зі змінами згідно наказу Адміністрації Держспецзв'язку від 13 травня 2021 року № 289: станом на 01 січня 2022 р. – Режим доступу

https://zakon.rada.gov.ua/laws/show/z0862-07#Text (дата звернення: 23.04.2025). – Назва з екрана.
52. Про ліцензування видів господарської діяльності [Електронний ресурс] : Закон України від 02 березня 2015 року від № 222-VIII : станом на 05 січня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/222-19#Text (дата звернення: 10.04.2025). – Назва з екрана.
53. Про деякі питання ліцензування господарської діяльності у галузі криптографічного захисту інформації (крім електронного цифрового підпису) та технічного захисту інформації за переліком, що встановлюється Кабінетом Міністрів України [Електронний ресурс] : Постанова КМУ від 16 листопада 2016 року № 821 : станом на 16 листопада 2016 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/821-2016-п#Text (дата звернення: 10.04.2025). – Назва з екрана.
54. Про електронні документи та електронний документообіг [Електронний ресурс] : Закон України від 22 травня 2003 року № 851- IV : станом на 31 грудня 2023 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 10.04.2025). – Назва з екрана.
55. ДСТУ 4163:2020 Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлювання : [Чинний з 2021-09-01]. – Київ : Держспоживстандарт України, 1996. – 37 с.
56. Типова інструкція з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади [Електронний ресурс] : Постанова КМУ від 17 січня 2018 року № 55 : станом на 17 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/55-2018-п#Text (дата звернення: 24.04.2025). – Назва з екрана.
57. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання [Електронний ресурс] : Наказ Міністерства юстиції України від 11 листопада 2014 року № 1886/5, зареєстровано в Міністерстві юстиції України 11 листопада 2014 року за № 1421/26198: станом на 10 травня 2025 р. – Режим доступу https://zakon.rada.gov.ua/laws/show/z1421-14#Text (дата звернення: 23.04.2025). – Назва з екрана.
58. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну [Електронний ресурс] : Постанова КМУ від 17 січня 2018 року № 55 : станом на 17 квітня 2025 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/55-2018-п#Text (дата звернення: 24.04.2025). – Назва з екрана.
59. Про електронну ідентифікацію та електронні довірчі послуги [Електронний ресурс] : Закон України від 05 жовтня 2017 року № 2155-VIII : станом на 18 грудня 2024 р. – Режим доступу:

https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 10.04.2025). – Назва з екрана.

60. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціями державної форми власності [Електронний ресурс] : Постанова КМУ від 01 серпня 2023 року № 798 : станом на 01 серпня 2023 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/798-2023-п#Text (дата звернення: 10.04.2025). – Назва з екрана.
61. Положення про державну експертизу у сфері криптографічного захисту інформації [Електронний ресурс] : Наказ Адміністрації Держспецзв'язку України від 23 червня 2008 року № 100, зареєстровано в Міністерстві юстиції України 16 липня 2008 року за № 651/15342 : станом на 02 грудня 2020 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0651-08#Text (дата звернення: 10.04.2025). – Назва з екрана.