

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

На правах рукопису
УДК 004.056.5

До захисту допущено
Завідувач кафедри ММСА
Оксана ТИМОЩУК
«__» _____ 2022 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 124 «Системний аналіз»

**на тему: «Системний підхід до процесу керування доступами в об'єктах
критичної інфраструктури в умовах воєнного стану»**

Виконав:
студент II курсу, групи КА-11мп
Пастушок Олена Олегівна _____

Керівник:
доцент кафедри ММСА,
д.т.н., доц. Тимощук Оксана Леонідівна _____

Рецензент:
доцент кафедри системного проектування
к.т.н., ст.н.с. Кисельов Г. Д. _____

Засвідчую, що у цій магістерській дисертації
немає запозичень з праць інших авторів без
відповідних посилань.

Студент _____

Київ
2022

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ**

Рівень вищої освіти – другий (магістерський)

Спеціальність – 124 «Системний аналіз»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Оксана ТИМОЩУК

«___» _____ 2022 р.

**ЗАВДАННЯ
на магістерську дисертацію студенту
Пастушок Олені Олегівні**

1. Тема дисертації: «Системний підхід до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану», науковий керівник роботи Тимощук Оксана Леонідівна, доцент кафедри ММСА, доктор технічних наук, затверджено наказом по університету №4046-с від «03» листопада 2022 р.
2. Термін подання студентом дисертації 12.12.2022
3. Об'єкт дослідження: стратегія керування доступом
4. Предмет дослідження: державні та міжнародні стандарти з інформаційної безпеки, а також методики розробки стратегії керування доступом
5. Перелік завдань, які потрібно розробити:
 - 1). Огляд актуальних державних стандартів з інформаційної безпеки (ІБ).
 - 2). Порівняння державних стандартів з сучасними міжнародними стандартами ІТ.

- 3). Визначення об'єктів критичної інфраструктури у відповідності до законодавства України.
- 4). Опис методології розробки системного підходу до процесу керування доступами.
- 5). Розробка системного підходу до процесу керування доступами.
6. Орієнтований перелік графічного (ілюстрованого) матеріалу: презентація
7. Орієнтований перелік публікацій: Тимощук О. Л. та Пастушок О. О. 'Системний підхід до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану'. 1-а Всеукраїнська Науково-практична конференція "Системний аналіз та інформатика", м. Київ, 22-29 листопада, 2022 року
8. Дата видачі завдання: 01.09.2022 _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів роботи	Примітка
1	Затвердження теми МД	01.09.2022-07.09.2022	виконано
2	Ознайомлення зі структурою МД згідно з Положенням про державну атестацію студентів НТУУ «КПІ ім. І. Сікорського»	08.09.2022-14.09.2022	виконано
3	Ознайомлення з ДСТУ 3008-2015 та стандартами ЄСПД	15.09.2022-21.09.2022	виконано
4	Проведення дослідження за темою МД під керівництвом керівника	22.09.2022-28.09.2022	виконано
5	Завершення роботи над першим варіантом частини МД	29.09.2022-05.10.2022	виконано
6	Проведення роботи над експериментальною частиною МД	06.10.2022-12.10.2022	виконано
7	Проведення роботи над програмним продуктом	13.10.2022-02.11.2022	виконано
8	Оформлення МД та аналіз отриманих результатів	03.11.2022-13.11.2022	виконано

Студент

Олена ПАСТУШОК

Керівник

Оксана ТИМОЩУК

РЕФЕРАТ

Магістерська дисертація має обсяг 93 сторінки, містить 23 рисунки, 21 таблицю та 18 посилань.

З кожним роком інформаційна безпека стає все більш ваговою частиною будь-якого підприємства, особливо критичної інфраструктури. Впровадження низки контролів та заходів для забезпечення захищеності інформації потребує великих вкладень та глибокого залучення співробітників зі сторони підприємства. Для ефективного провадження процесу керування доступами, все частіше застосовують методологію, що базується на поетапному впровадженні нормативної документації, технічних та управлінських рішень з інформаційної безпеки у процеси підприємства. Також цікавість до даної теми зумовлена тим, що велика кількість державних об'єктів критичної інфраструктури є потенційними цілями кібератак та потребує впровадження низки рішень з інформаційної безпеки, особливо під час воєнного стану.

Об'єктом дослідження є стратегія керування доступом.

Предметом дослідження є державні та міжнародні стандарти з інформаційної безпеки, а також методики розробки стратегії керування доступом.

Метою роботи є визначення застосовних державних стандартів до об'єктів критичної інфраструктури, порівняння державних та міжнародних стандартів ІБ, розробка систематичного підходу до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного часу.

Дана робота містить огляд на актуальні державні стандарти, визначення об'єктів критичної інфраструктури відповідно до чинного законодавства, порівняльний аналіз міжнародних та державних стандартів ІБ, операційну модель для оцінки стану ІБ підприємства, систематичний підхід до процесу керування доступом.

Ключові слова: критична інфраструктура, кібератаки, системний підхід, енергетичний сектор, ІТ стратегія, керування доступами.

Рік виконання кваліфікаційної магістерської роботи 2022. Рік захисту роботи 2022.

ABSTRACT

The master thesis has the volume of 93 pages, contains 23 figures, 21 tables and 18 references.

Every year, information security is becoming an increasingly important part of any enterprise, especially critical infrastructure. The implementation of a number of controls and measures to ensure information security requires large investments and deep involvement of employees on the part of the enterprise. For the effective implementation of the access management process, a methodology based on the phased introduction of regulatory documentation, technical and management solutions for information security into enterprise processes is increasingly being used. Also, interest in this topic is due to the fact that a large number of state critical infrastructure facilities are potential targets of cyberattacks and require the implementation of a number of information security solutions, especially during martial law.

The object of research is the access control strategy.

The subject of the research is state and international standards for information security, as well as methods of developing an access management strategy.

The purpose of the work is to determine applicable state standards for critical infrastructure facilities, compare state and international IS standards, develop a systematic approach to the process of access control in critical infrastructure facilities in wartime conditions.

This work contains an overview of current state standards, the definition of critical infrastructure objects in accordance with current legislation, a comparative analysis of international and state IS standards, an operational model for assessing the state of an enterprise's IS, a systematic approach to the access control process.

Key words: critical infrastructure, cyber attacks, system approach, energy sector, IT strategy, access control.

Year of qualifying master's thesis 2022. Year of defense of work 2022.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1	11
БЕЗПЕКА ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	11
1.1. Об’єкти критичної інфраструктури	11
1.2. Енергетичний сектор України під час військового стану.....	14
1.3. Забезпечення цілісності інформації критичної інфраструктури від кібератак	21
1.3.1. Вірус NotPetya	21
1.3.2. Вірус WannaCry.....	22
1.3.3. Вірус Stuxnet.....	23
1.3.4. Кібератака на «Укренерго».....	23
1.4. Процес керування доступами	25
Висновки до розділу 1	27
РОЗДІЛ 2	28
АНАЛІЗ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РОЗРОБКА ПРОЦЕСУ КЕРУВАННЯ ДОСТУПАМИ	28
2.1. Державні стандарти КСЗІ (Комплексні системи захисту інформації)	28
2.2. Міжнародні стандарти.....	29
2.2.1. Запит на доступ	30
2.2.2. Перевірка	31
2.2.3. Надання прав	31
2.2.4. Моніторинг стану ідентифікації.....	31
2.2.5. Доступ до реєстрації та відстеження	31
2.2.6. Видалення або обмеження прав доступу.....	32
2.3. ІТ Стратегія (Системний підхід до процесу керування доступами)..	33
2.3.1. Політики та процеси	34
2.3.2. Інвентаризація портфеля застосунків	35
2.3.3. Корпоративне управління	36
2.3.4. Визначення та задоволення потреб у доступі як зовнішніх та і внутрішніх користувачів.....	37

2.3.5. Визначення архітектури ІБ	38
2.3.6. Планування та використання суміжної технології IAM (Identity and Access Management).....	39
Висновки до розділу 2	40
РОЗДІЛ 3	41
СИСТЕМНИЙ ПІДХІД ДО ПРОЦЕСУ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ	41
3.1. Методика оцінки ризиків інформаційної безпеки	41
3.1.1. Класи активів і типи збитків.....	42
3.1.2. Сценарій реалізації загрози.....	42
3.2. Системний підхід до процесу керування доступом	46
3.3. Тест – приклад, який демонструє авторизацію в систему	53
Висновки до розділу 3	58
РОЗДІЛ 4	59
РОЗРОБКА ВЛАСНОГО СТАРТАП ПРОЕКТУ	59
4.1. План розробки стартапу та масштабування його на ринок	59
4.2. Опис ідеї стартап-проекту.....	61
4.3 Технологічний аудит ідеї проекту.....	62
4.4. Аналіз ринкових можливостей запуску стартап-проекту.....	64
4.5. Розроблення ринкової стратегії стартап-проекту	72
4.6. Розроблення маркетингової програми стартап-проекту	74
Висновки до розділу 4	77
ВИСНОВКИ.....	78
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	79
ДОДАТОК А.....	82
ПРЕЗЕНТАЦІЯ.....	82
ДОДАТОК Б	90
ЛІСТИНГ ПРОГРАМИ.....	90

ВСТУП

З кожним роком об'єкти критичної інфраструктури потерпають все більшої і більшої кількості кібератак, особливо під час воєнного стану. На сьогоднішній день в небезпеці знаходиться не тільки банківський сектор, а енергетичний, від якого залежить стабільність роботи всієї країни. Енергетика України перебуває у стані війни з 2014 року, тому з 24 лютого 2022 року, з повномасштабним вторгненням на територію України, певні рішення вже були відпрацьовані на територіях України, де раніше вели активні бойові дії та тимчасово окуповані території. Водночас, українська енергетика зустрілася з переліком нових, ще більш загрозливих викликів, як ядерний тероризм із захопленням АЕС, численні пошкодження критичної інфраструктури – електричних та газових мереж, критичне зниження попиту на енергетичні продукти у зв'язку з виїздом населення та припиненням бізнесу, ще більш критичне зниження рівня оплат в енергетичній системі, і рішення, незважаючи на бойові дії по всій території країни, продовжуватиме синхронізацію енергетичної системи України з енергосистемою Континентальної Європи, паливну кризу тощо. Окрім, всього вищесказаного енергетичний сектор попав під вплив хактивістів та кіберзлочинців, які намагаються розхитати енергетичну структуру з середини [1].

Метою даної роботи є дослідження державних стандартів, які регламентують захист об'єктів критичної інфраструктури від кіберзагроз з подальшим порівнянням їх з міжнародними стандартами інформаційної безпеки, та розробкою:

- системного підходу до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану;
- методики оцінки зрілості;
- тестовий приклад процесу керування доступами.

Об'єктом дослідження є стратегія керування доступом.

Предметом дослідження є державні та міжнародні стандарти з інформаційної безпеки, а також методики розробки стратегії керування доступом.

Методи дослідження: аналіз актуальних державних та міжнародних стандартів інформаційної безпеки; проведення аналізу робіт з розробки стратегії процесу керування доступом на підприємствах критичної інфраструктури.

Наукова новизна роботи полягає в розробці системного підходу до процесу керування доступом в об'єктах критичної інфраструктури в умовах воєнного стану, що поєднує в собі найкращі практики міжнародних стандартів та виконання вимог державних стандартів.

Практичне значення роботи полягає у розробці системного підходу, методик оцінки стану підприємства та розробки тестового прикладу, який демонструє надійний захист, що забезпечує конфіденційність, цілісність та доступність інформації критичної інфраструктури. Розроблені рішення покликані спростити процес керування доступами для об'єктів критичної інфраструктури та підвищити рівень якості впровадження рішень інформаційної безпеки.

РОЗДІЛ 1

БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Об'єкти критичної інфраструктури

Згідно із законом України «Про критичну інфраструктуру» [1], всі об'єкти критичної інфраструктури повинні відповідати поставленим у законі вимогам інформаційної безпеки. Таким чином, згідно пункту 13 Статті 1 [1] об'єктами критичної інфраструктури є об'єкти, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. В Україні до об'єктів критичної інфраструктури відносяться компанії та установи з таких галузей, як енергетика, хімічна промисловість, транспорт, банківська справа та фінанси, інформаційні технології та телекомунікації (електронний зв'язок), харчування, охорона здоров'я, комунальне господарство, які є стратегічно важливими для функціонування економіки та безпеки держави, суспільства і населення, виведення з ладу або знищення яких може вплинути на національну безпеку і оборону, навколишнє природне середовище, призвести до значних матеріальних і фінансових втрат, людських втрат [2].

Загальна ціль Закону України «Про критичну інфраструктуру», який був підписаний 10 грудня Президентом України, регулювання захисту підприємств та організацій, які мають велике значення для життєвого функціонування країни, а також які вимагають особливої уваги до захисту такої інфраструктури від природних і техногенних катастроф (починаючи від повеней та посухи до кібератак, військових дій та терористичних актів). Чому це було зроблено? Яскравим прикладом цього може слугувати відключення електрики, або різке зникнення мобільного зв'язку чи, наприклад, зупиниться поставка харчової продукції. Також, технологічним прикладом може бути

кібератака NotPetya здійснена в 2017 році [3]. Під час даної кібератаки було призупинено роботу великої кількості компаній.

При цьому виявилось, що в нашій країні немає особливих вимог щодо безпеки об'єктів критичної ваги, немає навіть поняття «об'єкти критичної інфраструктури».

При цьому самі вимоги безпеки, у тому числі кібербезпеки, були чітко розроблені та прописані лише для банківського сектора відповідно до міжнародних стандартів. Є певні вимоги і до державного сектору, але, знову ж таки, лише у сфері інформаційної безпеки, вони сильно застаріли. Всі інші галузі економіки, що існують насправді, нічим не регулюються.

Перша згадка терміна «об'єкти критичної інфраструктури» пов'язана з його появою у Законі України «Про основні засади кібербезпеки України» у 2018 році, яким встановлено, що такі об'єкти існують, а також затверджено методику класифікації та перелік таких об'єктів. формується Кабінетом Міністрів України та Національним банком України (але лише для банківського сектору). Таким чином відповідно до статті 9 даного закону було окреслено 17 секторів економіки, які були віднесені до критичної інфраструктури [1]:

1. Енергозабезпечення (в даному пункті також враховується постачання теплої енергії).
2. Охорона здоров'я.
3. Водопостачання та водовідведення.
4. Надання адміністративних послуг та урядування.
5. Продовольче забезпечення.
6. Фармацевтична промисловість.
7. Дослідницька діяльність.
8. Виготовлення вакцин та функціонування біолабораторій.
9. Хімічна промисловість.
10. Інформаційні послуги.

11. Космічні технології та послуги, а також космічна діяльність.
12. Електронні комунікації.
13. Служби порятунку та цивільний захист населення та територій.
14. Фінансові послуги.
15. Державна безпека та оборона.
16. Транспортне забезпечення.
17. Тримання під вартою, правопорядок та здійснення правосуддя.

Але навіть даний список не є повним, оскільки у формулюванні закону використовується фраза «в тому числі».

Крім того, у статті 10 [1] зазначено, що під такими об'єктами можуть розташовуватись організації не лише республіканського, а й місцевого значення залежно від ступеня критичності:

I категорія критичності - особливо важливі об'єкти загальнодержавного значення, що суттєво впливають на інші об'єкти критичної інфраструктури, і порушення їх функціонування призведе до виникнення кризової ситуації загальнодержавного значення;

II категорія критичності - життєво важливі об'єкти, вихід із ладу яких призведе до виникнення кризової ситуації регіонального значення;

III категорія критичності - важливі об'єкти, вихід із ладу яких призведе до виникнення кризової ситуації місцевого значення;

IV категорія критичності - необхідні об'єкти, вихід із ладу яких призведе до виникнення кризової ситуації місцевого значення.

Таким чином, під регулювання потрапить безліч об'єктів різного рівня — від електростанцій до місцевого продуктового магазину, який є єдиним у віддаленому селищі.

1.2. Енергетичний сектор України під час військового стану

Енергетика України перебуває у стані війни з 2014 року, тому з 24 лютого 2022 року, з повномасштабним вторгненням на територію України, певні рішення вже були відпрацьовані на територіях України, де раніше вели активні бойові дії та тимчасово окуповані території. Водночас, українська енергетика зустрілася з переліком нових, ще більш загрозливих викликів, як ядерний тероризм із захопленням АЕС, численні пошкодження критичної інфраструктури – електричних та газових мереж, критичне зниження попиту на енергетичні продукти у зв'язку з виїздом населення та припиненням бізнесу, ще більш критичне зниження рівня оплат в енергетичній системі, і рішення, незважаючи на бойові дії по всій території країни, продовжуватиме синхронізацію енергетичної системи України з енергосистемою Континентальної Європи, паливну кризу тощо. Набуття Україною статусу кандидата на вступ до ЄС ставить додаткові виклики енергетиці та регулюванню цієї галузі.

У сфері енергетики з 24 лютого 2022 року було запроваджено низку регуляторних змін, покликаних стабілізувати галузь та вирішити критичні проблеми. Цей процес продовжується, оскільки очікується, що опалювальний сезон 2022/2023 буде надзвичайно складним [4].

Експорт електроенергії. З 16 березня 2022 року Енергетична Система Континентальної Європи та Об'єднана енергетична система (далі – ОЕС) України працюють синхронно. 30 червня почалися комерційні продажі електроенергії в країни ЄС на рівні 100 МВт (Румунія, і пізніше до Словаччини). З 30 липня обсяг збільшено до 250 МВт, на додаток до експорту 210 МВт до Польщі. В даний час ОСП здійснює розподіл пропускної спроможності міждержавних зв'язків до країн ЄС на добових аукціонах. Надалі термін планується збільшити (тиждень, місяць, квартал).

Водночас, Уряд поклав спеціальні обов'язки експортерів електроенергії до країн-членів ЄС протягом дії воєнного стану (ухвала № 775 від 07.07.2022 року) [5]. За цим механізмом експортери платять гарантованому покупцю за послугу забезпечення безпеки постачання електричної енергії. Вартість послуги складає 80% доходів експорту електроенергії. З доходів виключаються витрати експортерів на послуги диспетчерського управління, передачі електроенергії, витрати на доступ до фізичного права на передачу пропускної спроможності з обох боків кордону. При цьому прибуток експортера існує у разі позитивної різниці між ціною на ринках "на добу вперед" країни-імпортера та України за відповідний розрахунковий місяць. Таке фінансове навантаження на експортерів не знизило зацікавлення аукціонами Укренерго щодо розподілу потужності міждержавних зв'язків.

Зберігання електричної енергії. Законодавчі зміни, що врегулювали діяльність зі зберігання енергії на ринку електричної енергії, прийняті 15 лютого 2022 р. (закон № 2046-IX) [6], а набули чинності 16 червня 2022 р. Така діяльність підлягає ліцензуванню та здійснюється оператором установки зберігання енергії, та у виняткових випадках може здійснюватися без ліцензії виробниками, споживачами, операторами систем передачі та розподілу. 22 липня 2022 р. НКРЕКУ затверджено Ліцензійні умови провадження господарської діяльності зі зберігання енергії (ухвала № 798) [7]. Ліцензуванню підлягає діяльність, якщо сумарна встановлена потужність установок зберігання енергії становить 150 кВт та вище. При цьому забороняється одночасно здійснювати діяльність зі зберігання енергії та передачі та розподілу електричної енергії, транспортування та розподілу газу, виконання функцій оператора ринку та гарантованого покупця. Врегулювання діяльності зі зберігання енергії є довгоочікуваним на ринку, оскільки українська ОЕС потребує додаткових інструментів гнучкості.

Покладання спеціальних обов'язків (далі – ПСО) над ринком електричної енергії. Додатково до ПСО на експортерів, описаного вище,

змінами до урядової постанови про ПСО № 483 від 5 червня 2019 р. до 31 жовтня 2022 р. продовжено дію фіксованих цін за 1 кВт електричної енергії для побутових споживачів на рівні 1,44 грн (обсяг споживання до 250 кВт) та 1,68 грн (понад 250 кВт год). Крім того, уряд постановою № 838 від 22 липня 2022 р. застосував механізм ВСО до Укренерго, яким зобов'язав надати цільову безвідсоткову зворотну допомогу ДП "Укрвугілля" на суму, необхідну для придбання вугільної продукції обсягом до 1 млн. тон за ринковою ціною, але не більше 2,5 млрд гривень, для потреб виробників електричної енергії, які експлуатують ТЕС та ТЕЦ. Допомога має бути повернена до 1 червня 2023 року.

Інші системні зміни на ринку електричної енергії: 29 липня 2022 р. Верховна Рада України ухвалила Закон «Про особливості регулювання відносин на ринку природного газу та у сфері теплопостачання під час дії військового стану та подальшого відновлення їх функціонування» (Законопроект № 7427 від 01.06. 2022) [8], яким також врегульовано зміни на ринку електричної енергії. Закон перебуває на підписі у Президента України. Основні зміни, передбачені Законопроектом № 7427:

- виробникам з ВЗЕ надано право тимчасово виходити з балансуєної групи гарантованого покупця. Крім того, виробникам із ВЗЕ, які не отримують стимулювання (наприклад, «зеленого» тарифу), надано право укласти зі споживачем договір про надання послуги із забезпечення стабільності ціни на електричну енергію (за цим договором виробник придбає у споживача послугу, якщо ціна на електричну енергію на ринку України перевищує верхній рівень встановленого сторонами показника, а споживач придбає у виробника послугу, якщо ціна на електричну енергію на ринку України нижча за нижній рівень відповідного показника). Ці інструменти стимулюють виробників ВЗЕ працювати на ринкових засадах, без державної підтримки у вигляді зеленого тарифу;

- до 1 квітня 2023 року продовжено зобов'язання виробників здійснювати продаж електричної енергії за двосторонніми договорами виключно на електронних аукціонах. Важливо також уточнити, чи ця вимога поширюється на експортні договори;
- змінено цільове спрямування коштів, отриманих оператором системи передачі (далі – ОСП) від розподілу пропускної спроможності міждержавного перетину, а саме кошти, отримані станом на 31 липня 2022 року, використовуються для таких цілей: (I) 10% на технічне обслуговування та інвестиції у систему передачі, погашення заборгованості за договорами щодо доступу до пропускної спроможності міждержавного перетину; (II) 45% на погашення заборгованості ОСП на ринку, що балансує. Виробники, що експлуатують ТЕС та ТЕЦ, зобов'язані спрямувати такі кошти на закупівлю палива або на проведення ремонтних робіт для забезпечення опалювального сезону 2022/23 років; (III) 45% – на погашення заборгованості ОСП перед гарантованим покупцем у рамках вибухобезпечного механізму (ВЗГ). Гарантований покупець зобов'язаний перерахувати такі кошти атомної та зеленої генерації пропорційно до заборгованості. Кошти, отримані ОСП від розподілу пропускної спроможності міждержавного перетину з 1 серпня 2022 року до 1 січня 2023 року, використовуються для таких цілей: (I) 50% на погашення заборгованості ОСП на ринку, що балансує; (II) 50% – на погашення заборгованості ОСП за механізмом ВЗГ (вибухобезпечний) для ВДЕ. Цей механізм покликаний покращити фінансовий стан на ринку;
- до 31 грудня 2023 року продовжено термін, протягом якого функції постачальника «останньої надії» покладаються без проведення конкурсу, та до 1 липня 2023 року продовжено термін для проведення конкурсу на вибір постачальників універсальних послуг.

Мораторій на підвищення цін (тарифів) на ринку природного газу та у сфері теплопостачання: Законопроект № 7427 передбачає наступні зміни на ринку газу, введені на період дії військового стану в Україні та протягом шести місяців після його припинення/скасування:

- забороняється підвищення тарифів на послуги з розподілу газу; теплову енергію (її виробництво, транспортування та постачання) та послуги з постачання теплової енергії та постачання гарячої води;
- ціна на природний газ для побутових споживачів, а також для ОСББ, житлово-будівельних кооперативів, іншої уповноваженої співвласниками особи, виробників теплової енергії, якщо вони використовують природний газ для виробництва теплової енергії для населення, не підлягає збільшенню від ціни станом на 24 лютого 2022;
- постачальнику газу забороняється здійснювати будь-які дії з примусу побутового споживача до оплати заборгованостей;
- законодавчо гарантована компенсація учасникам ринку, які забезпечують виконання заходів щодо введеного мораторію на підвищення цін (тарифів). Ці зміни необхідні соціального захисту населення період опалення.

Експорт/зберігання газу. З початком повномасштабного вторгнення учасникам ринку природного газу було заборонено здійснювати експорт природного газу з митної території України, зокрема природного газу в газосховищах України у митному режимі "митний склад" (наказ Міненерго №99 від 03.03.2022 р.) [9]. Через місяць цю норму було змінено та дозволено реекспорт природного газу, ввезеного на митну територію України для зберігання у митному режимі митного складу. Пізніше цей наказ Міненерго було скасовано через урядову заборону на експорт природного газу українського походження. Відповідно до постанови КМУ №666 від 10.06.2022р. квота експорту встановлена на рівні 0, як і для вугілля та мазуту,

що пов'язано з необхідністю сформувати ресурс для проходження осінньо-зимового опалювального сезону в Україні.

Запуск обороту біометану. Уряд затвердив Порядок функціонування реєстру біометану (ухвала № 823 від 22.07.2022 р.). Відповідно до цього Порядку Держенергоефективності є органом, відповідальним за ведення Реєстру біометану та видачу гарантій походження та сертифікатів походження біометану. Саме ці документи підтверджують, що біометан виготовлений з біомаси, тобто є відновлюваним газом. Крім того, НКРЕКУ шляхом внесення змін до Кодексу газотранспортної системи та Кодексу газорозподільних систем, врегулювала питання постачання біометану в газові мережі, для цього збільшено максимально допустимий рівень вмісту кисню в природному газі з 0,02 мл. % до 0,2мл. % для доступу до газотранспортної системи та до 1,0 мл. % для доступу до газорозподільних систем (постанова НКРЕКУ № 847 від 02.08.2022 р.). Ухвалені рішення дозволяють імплементувати загальні умови обігу біометану, визначені Законом України «Про альтернативні види палива», запустити ринок біометану в Україну та можливість його експорту до ЄС.

ВЗГ. З 1 березня постановою КМУ №222 від 06.03.2022 р. на учасників ринку газу покладено спеціальні обов'язки для забезпечення суспільних інтересів у процесі функціонування ринку природного газу. Механізм, який надалі зазнавав змін, передбачає пільгові умови для:

- побутових споживачів: постачальники повинні укласти договір з ТОВ “Газопостачальна компанія “Нафтогаз Трейдинг”, щоб забезпечити своїх побутових споживачів газом за ціною базової річної пропозиції такого постачальника, який діяв на 24 лютого 2022 року. Такий механізм забезпечення споживачів діятиме до 30 вересня 2022 року.
- операторів газорозподільних систем: вони купують газ у ТОВ “ГК “Нафтогаз України”, в обсязі:

- нормативних та виробничо-технологічних витрат за ціною 7420 грн за 1 тис. м3;
- втрат, спричинених воєнними діями та заподіяних у зв'язку із запобіганням/урегулюванню гуманітарних кризових ситуацій, за ціною 0,01 грн за 1 тис. м3;
- понаднормових втрат та виробничо-технологічних витрат за ціною, що розраховується за формулою на підставі спотових цін на ринку газу Словаччини та з урахуванням вартості транспортування газу зі Словаччини до України. Механізм діятиме під час військового стану та протягом шести місяців після його припинення/скасування;
- непобутових споживачів, які виконують життєво важливі функції для забезпечення обороноздатності держави (згідно з переліком; крім споживачів на тимчасово окупованій території України): постачання природного газу постачальником останньої надії здійснюється за ціною 32 тис. грн за 1 тис. м3. Механізм діє до 30 вересня 2022 р.
- виробників теплової енергії: НАК "Нафтогаз України" придбає у АТ "Укргазвидобування" та ДАТ "Чорноморнафтогаз" природний газ за ціною 7 240 грн. за 1 тис. м3 для формування ресурсу природного газу для побутових споживачів та виробників теплової енергії для подальшого забезпечення виконання ТОВ "ДК "Нафтогаз Трейдинг" зобов'язань щодо постачання газу за довгостроковими контрактами з виробниками теплової енергії. Механізм діє до 30 вересня 2022 р.

Виклики, які постали перед Україною у зв'язку з повномасштабними воєнними діями на території нашої країни, особливо відчутні та серйозні для енергетичної сфери. Це стосується як оперативного відновлення інфраструктурних об'єктів від руйнувань, завданих військовими діями, так і забезпечення проходження осінньо-зимового опалювального періоду 2022/2023 років, що очікується найскладнішим для всього Європейського

континенту, а також стратегічним відновленням та оновленням енергетичної галузі в контексті придбання Україною статус кандидата на вступ до Євросоюзу. Очікується, що не кожен виклик, і не з першого разу можна знайти оптимальну відповідь. Однак важливо правильно визначити та зафіксувати стратегічні пріоритети, а також їх фінансово-економічні можливості та джерела, щоб розвиток нормативного регулювання енергетики був максимально прогнозованим та прозорим для всіх учасників енергетичних ринків.

1.3. Забезпечення цілісності інформації критичної інфраструктури від кібератак

Кіберзлочинність може порушити й завдати шкоди бізнесу підприємства. Наприклад, у 2021 році середня вартість витоку даних становила 4,24 мільйона доларів США у всьому світі та 9,05 мільйона доларів США у США. Ці витрати включають виявлення порушення та реагування на нього, вартість простою та втрату доходу, а також довгострокову репутаційну шкоду бізнесу та його бренду. А у випадку скомпрометованої ідентифікаційної інформації це може призвести до втрати довіри клієнтів, штрафних санкцій і навіть судового позову [10].

1.3.1. Вірус NotPetya

Petya використовує вразливість CVE-2017-0144 у реалізації Microsoft протоколу Server Message Block. Після використання вразливості ця атака шифрує основний завантажувальний запис серед інших файлів. Він надсилає користувачеві повідомлення про перезавантаження системи, після чого

система стає недоступною. Це робить операційну систему нездатною знаходити файли, і немає способу розшифрувати файли, що робить Petya очисником, а не програмою-вимагачем, якою її спочатку вважали.

Новий варіант ще більше розширив свої можливості, додавши механізм розповсюдження, подібний до того, що ми бачили в WannaCry у травні 2017 року. 14 березня корпорація Майкрософт випустила набір критичних патчів, щоб усунути основну вразливість у підтримуваних версіях Windows, але багато організацій можливо, ще не застосували ці виправлення.

Зловмисне програмне забезпечення Petya існує вже досить давно, а атака в червні 2017 року запустила новий варіант. Цей варіант деякі називають NotPetya через зміни в поведінці зловмисного програмного забезпечення. Petya та NotPetya використовують різні ключі для шифрування та мають унікальні стилі перезавантаження, відображення та нотатки. Проте обидва однаково руйнівні [3].

1.3.2. Вірус WannaCry

У травні 2017 року програма-вимагач WannaCry поширилася по всьому світу через комп'ютери під керуванням Windows. Майже два місяці тому Microsoft випустила патч безпеки для EternalBlue, експлойта, який зловмисники використовували для поширення програми-вимагача WannaCry. Однак багато користувачів Windows у всьому світі не оновили своє програмне забезпечення або використовували застарілі версії Windows, тому були вразливі до великомасштабної атаки.

Зловмисники WannaCry шифрували комп'ютери Windows по всьому світу та вимагали викуп у розмірі спочатку 300 доларів у біткойнах, пізніше – у 600 доларів. Він заразив близько 230 000 комп'ютерів у 150 країнах всього за кілька годин. Після того, як атака спочатку швидко поширилася по всьому

світу, дослідник безпеки Маркус Хатчінс виявив вимикач, який значно сповільнив поширення атаки [11].

1.3.3. Вірус Stuxnet

Stuxnet знищив численні центрифуги на іранському заводі зі збагачення урану в Натанзі, змусивши їх згоріти. Згодом інші групи модифікували вірус, щоб націлити його на об'єкти, зокрема очисні станції, електростанції та газопроводи.

Stuxnet був багатокомпонентним хробаком, який подорожував на USB-накопичувачах і поширювався через комп'ютери Microsoft Windows. Вірус шукав на кожному зараженому комп'ютері ознаки програмного забезпечення Siemens Step 7, яке промислові комп'ютери, що служать ПЛК, використовують для автоматизації та моніторингу електромеханічного обладнання. Після виявлення комп'ютера з ПЛК зловмисне програмне забезпечення оновило його код через Інтернет і почало надсилати інструкції, що викликають пошкодження, до електромеханічного обладнання, яким керував ПК. При цьому вірус надсилав головному контролеру помилковий відгук. Будь-хто, хто спостерігав за обладнанням, не мав би ознак проблеми, доки обладнання не почало самознищуватися [12].

1.3.4. Кібератака на «Укренерго»

Диспетчери всередині диспетчерської Національної енергетичної компанії України «Укренерго» в Києві, Україна, 13 жовтня 2016 року. Коли 17-18 грудня на півночі Києва зникло світло, енергопостачальник "Укренерго"

запідозрив кібератаку та найняв слідчих, щоб допомогти встановити причину після серії зломів по всій Україні.

Попередні висновки вказують на те, що робочі станції та системи диспетчерського контролю та збору даних (SCADA), пов'язані з 330-кіловатною підстанцією «Північна», зазнали впливу зовнішніх джерел поза межами нормальних параметрів, йдеться в коментарях Укренерго, надісланих Reuters електронною поштою.

«Аналіз впливу симптомів на вихідні дані цих систем свідчить про сплановане та багаторівневе вторгнення», – заявили в «Укренерго».

Співробітники правоохоронних органів і кіберексперти все ще працюють над складанням хронології подій, складанням списку зламаних облікових записів і визначенням точки проникнення, одночасно відстежуючи комп'ютери, потенційно заражені шкідливим програмним забезпеченням у режимі сну, йдеться в повідомленні.

У коментарях не згадується, яка особа, група чи країна могла стояти за нападом.

«Це був навмисний кіберінцидент, який не мав на меті великого масштабу... вони насправді атакували більше, але не змогли досягти всіх своїх цілей», — сказала Марина Кротофіл, провідний дослідник кібербезпеки Honeywell, яка допомагала в розслідуванні.

У грудні 2015 року перша у своєму роді кібератака позбавила світла 225 000 людей на заході України, а хакери також саботували обладнання для розподілу електроенергії, ускладнюючи спроби відновити електропостачання. Українські спецслужби поклали відповідальність за атаку на Росію.

Вважається, що під час останньої атаки хакери непомітно ховалися в ІТ-мережі Укренерго протягом шести місяців, отримуючи привілеї доступу до систем і з'ясовуючи їхню роботу, перш ніж вжити методичних заходів для відключення електроенергії, сказав Кротофіл.

«У команді, яка була задіяна, працювало досить багато людей, які володіли дуже серйозними інструментами та інженером, який розуміється на енергетичній інфраструктурі», — сказала вона.

Атаки на енергомережу України широко розглядаються експертами як перші приклади того, як хакери відключили критично важливі енергетичні системи, що постачають тепло та світло мільйонам домівок [13].

1.4. Процес керування доступами

Контроль доступу є фундаментальним компонентом безпеки даних, який визначає, кому дозволено отримувати доступ і використовувати інформацію та ресурси компанії. Завдяки автентифікації та авторизації політики контролю доступу гарантують, що користувачі є тими, за кого себе видають, і що вони мають відповідний доступ до даних компанії. Контроль доступу також можна застосувати для обмеження фізичного доступу до кампусів, будівель, кімнат і центрів обробки даних [14].

Контроль доступу ідентифікує користувачів шляхом перевірки різних облікових даних для входу, які можуть включати імена користувачів і паролі, PIN-коди, біометричні скани та маркери безпеки. Багато систем контролю доступу також включають багатофакторну автентифікацію (MFA), метод, який вимагає кількох методів автентифікації для перевірки особи користувача. Після автентифікації користувача система керування доступом авторизує відповідний рівень доступу та дозволені дії, пов'язані з обліковими даними та IP-адресою цього користувача.

Існує чотири основних типи контролю доступу. Організації зазвичай обирають метод, який є найбільш доцільним на основі їхніх унікальних вимог до безпеки та відповідності. Чотири моделі контролю доступу [14]:

- Дискреційне керування доступом (DAC): у цьому методі власник або адміністратор захищеної системи, даних або ресурсу встановлює правила для того, кому дозволено доступ.
- Обов'язковий контроль доступу (MAC): у цій недискреційній моделі людям надається доступ на основі дозволу інформації. Центральний орган регулює права доступу на основі різних рівнів безпеки. Ця модель поширена в урядових і військових середовищах.
- Контроль доступу на основі ролей (RBAC): RBAC надає доступ на основі визначених бізнес-функцій, а не ідентифікаційних даних окремого користувача. Мета полягає в тому, щоб надати користувачам доступ лише до тих даних, які вважаються необхідними для виконання їхніх ролей в організації. Цей широко використовуваний метод базується на складній комбінації призначень ролей, повноважень і дозволів.
- Контроль доступу на основі атрибутів (ABAC): у цьому динамічному методі доступ ґрунтується на наборі атрибутів і умов навколишнього середовища, таких як час доби та місцезнаходження, призначених користувачам і ресурсам.

Контроль доступу запобігає потраплянню конфіденційної інформації, такої як дані клієнтів, особиста інформація та інтелектуальна власність, у чужі руки. Це ключовий компонент сучасної системи безпеки з нульовою довірою, яка використовує різні механізми для постійної перевірки доступу до мережі компанії. Без надійної політики контролю доступу організації ризикують витоком даних із внутрішніх і зовнішніх джерел.

Контроль доступу особливо важливий для організацій із гібридною хмарою та багатохмарним середовищем, де ресурси, програми та дані зберігаються як локально, так і в хмарі. Контроль доступу може забезпечити ці середовища більш надійною безпекою доступу, окрім єдиного входу (SSO), і запобігти

несанкціонованому доступу з некерованих пристроїв і пристроїв BYOD (Bring Your Own Device) [14].

Висновки до розділу 1

У даному розділі було описано об'єкти критичної інфраструктури їх категоризацію та класифікацію, а також було розглянуто чотири ступеня критичності об'єктів інфраструктури.

Також, було розглянуто декілька успішних кібератак, які принесли збитки для сектору критичної інфраструктури, а також способи їх реалізації.

Розглянули важливість процесу керування доступами і дійшли висновку, що контроль доступу захищає дані та критичну інформацію від несанкціонованого доступу та неавторизованих дій.

РОЗДІЛ 2

АНАЛІЗ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РОЗРОБКА ПРОЦЕСУ КЕРУВАННЯ ДОСТУПАМИ

2.1. Державні стандарти КСЗІ (Комплексні системи захисту інформації)

Зазвичай об'єкти критичної інфраструктури зберігають інформацію, яка є конфіденційна, в більшості випадків дана інформація є власністю держави, але в поодиноких випадках це може бути приватна власність, тому розробка процесу управління доступами до даної інформації повинна відповідати регламентованим вимогам КСЗІ.

У державній власності є низка документів, які регламентують комплексні системи захисту інформації (КСЗІ), етапи та створення. Для процесу управління доступами загальним документом, який забезпечує організаційно-технічні положення та вимоги є ДСТУ 2155-93 чинний від 01.01.1995 року [15]. Усі вимоги, які зазначені в даному документі є обов'язковими для енергетичних об'єктів та підлягає технічному захисту. Також виконання вимог стандарту 3396.0-96 (чинного від 01.01.1997 року) визначає порядок проведення робіт для створення КСЗІ є – ДСТУ 3396.1-96 [16]. Вимоги цього стандарту є обов'язковими для підприємств та установ, в залежності від рівня їх важливості для забезпечення окремих життєво важливих функцій, в межах секторів критичної інфраструктури.

Проаналізувавши вимоги державних стандартів було з'ясовано що відповідно до ДСТУ 3369.0-96 встановлено такий порядок проведення робіт для створення КСЗІ:

- Проведення обстеження підприємства, установи організації, визначення та аналіз загроз.
- Розроблення системи захисту інформації.

- Реалізація плану захисту інформації.
- Контроль функціонування та керування системою захисту інформації.

2.2. Міжнародні стандарти

Управління доступом в організації — це перевага того, наскільки добре організація функціонує, коли йдеться про авторизацію активів для користувачів. Проблемний аспект неавторизованого доступу усувається завдяки ефективному управлінню доступом у будь-якій організації. Для регулювання та створення ефективного процесу управління доступами в ІТ системах існує декілька міжнародних стандартів. Найбільш використовуваними міжнародними стандартами є CISCO Benchmarks та ITIL. Відповідно даних стандартів доступ – це обсяг функціональних можливостей служби чи активу, якими певний користувач має право використовувати. Управління доступом до ITIL — це процес, відповідальний за надання доступу лише авторизованим користувачам до певних активів та ІТ-служб, одночасно запобігаючи доступу неавторизованих користувачів [17]. Основною метою керування доступом ITIL це є захистити дані від доступу неавторизованих користувачів. Це надзвичайно важливо для організації, оскільки потрапляння критично важливих даних у чужі руки може завдати компанії незворотної шкоди.

Відповідно стандарту ITIL процес управління доступами виглядає наступним чином (див. Рис. 2.1):



Рисунок 2.1 - Процес управління доступом відповідно ITIL.

2.2.1. Запит на доступ

Першим кроком є запит на доступ до певної ІТ-послуги, надіславши один із наведених нижче типів запитів:

- стандартний запит був відправлений безпосередньо з відділу кадрів;
- запит на зміну надсилається з процесу керування змінами;
- від служби обслуговування надійшов запит на обслуговування;
- запит на автоматичне надання, де менші запити обробляються автоматично.

2.2.2. Перевірка

Обов'язком управління доступом є перевірити особу користувача, який робить запит, і законність зробленого запиту.

2.2.3. Надання прав

Після перевірки особи користувача управління доступом надає йому право доступу до певної ІТ-послуги згідно з правилами, визначеними в Стратегії надання послуг ITIL. Якщо не визначено, керування доступом надає користувачеві права доступу до служби після надсилання запитів у відповідні відділи та отримання схвалення.

2.2.4. Моніторинг стану ідентифікації

У великій організації відбувається постійна зміна співробітників на певній посаді або тих, хто запитує доступ до ІТ-служб. Обов'язком управління доступом є відстеження всіх прав доступу, наданих різним співробітникам, і оновлення їх, коли відповідні працівники більше не займають цю посаду.

2.2.5. Доступ до реєстрації та відстеження

Керування доступом також має вести постійний контроль за користувачами ІТ-послуг, яким надано доступ. Необхідно контролювати всі дії процесів роботи служби, щоб гарантувати, що лише користувачі з

відповідним дозволом і авторизацією мають доступ до певної ІТ-послуги. Вони також повинні визначити параметри, які полегшують виявлення вторгнень у систему неавторизованих користувачів, надлишкових неправильних спроб входу та незвичних дій.

2.2.6. Видалення або обмеження прав доступу

Необхідно контролювати права доступу користувача, щоб, коли роль користувача змінюється протягом певного періоду часу, і йому більше не потрібен доступ до раніше необхідної ІТ-послуги, дозвіл на доступ має бути скасовано. Залежно від поточного статусу користувача, його доступ необхідно обмежити або припинити відповідно.

Управління доступом забезпечує для бізнесу такі цінності:

- Це гарантує збереження конфіденційності інформації шляхом контролю доступу до різних ІТ-сервісів.
- Гарантує, що працівники мають лише необхідний рівень доступу для ефективного виконання своєї роботи.
- Зменшує ймовірність виникнення помилки під час використання важливої служби, не дозволяючи некваліфікованим користувачам отримати до них доступ.
- Він надає засоби перевірки ІТ-служб і відстеження будь-якого зловживання послугами.
- Гарантує, що доступ до служби для певного користувача може бути скасований, коли це необхідно для дотримання вимог безпеки.

Таким чином, керування доступом успішно захищає дані від доступу неавторизованих користувачів, що надзвичайно важливо для організації. Це

запобігає потраплянню критично важливих даних у чужі руки та запобігає збитку компанії [17].

2.3. IT Стратегія (Системний підхід до процесу керування доступами)

IT-стратегія — це комплексний план, який визначає, як слід використовувати технології для досягнення цілей IT і бізнесу. Це схема того, як технології можуть підтримувати вашу загальну бізнес-стратегію. Він охоплює всі аспекти управління технологіями, включаючи управління вартістю, обладнанням і програмним забезпеченням, управління постачальниками та управління ризиками [18].

Спираючись на міжнародні та державні стандарти з приводу процесу керування доступами пропоную розробити системний підхід до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану, який допоможе забезпечити необхідний рівень інформаційної безпеки в поєднанні з бізнес-процесами.

Стратегія керування доступом включає в себе наступні ключові аспекти, які потрібно виконувати для досягнення цілі: політики, процеси ІБ, інвентаризація портфеля застосунків, корпоративне управління, визначення та задоволення потреб у доступі як зовнішніх та і внутрішніх користувачів, визначення архітектури ІБ, планування та використання суміжної технології IAM (Identity and Access Management).

У наступних розділах більш детально описано всі складові стратегії керування доступом та описані етапи, які необхідно виконувати при аналізі кожної складової.

2.3.1. Політики та процеси

Процес аналізу стратегії керування доступом як і інший процес ІБ розпочинається з нормативної бази документів та процесів ІБ, а також з оцінки рівня зрілості даних процесів. Даний етап є обов'язковим для того щоб розуміти на якому рівні знаходиться процес на даний момент. Аналіз існуючої нормативно-правової бази включає наступні етапи:

1. Зібрати перелік розроблених підприємством документів та їх номенклатуру;
2. Проаналізуйте поточну політику та процедури, пов'язані з інформаційною безпекою, а саме процесом керування доступом;
3. Проаналізувати нормативні документи, базові норми та правила для відповідності вимогам регуляторного органу та кращим практикам (вимоги НБУ, вимоги підприємства до критичної інфраструктури, рекомендації ISO, передові практики ITIL);
4. Визначити відсутні документи та розробити перелік пропозицій щодо доповнення існуючої нормативної бази.

Наступним етапом є оцінка рівня зрілості встановлених у компанії процесів керування доступом. Для цього необхідно виконати певний перелік дій, а саме:

1. Проаналізуйте ключові процеси керування доступом;
2. Оцініть поточну зрілість процесу та поведінки ІБ;
3. Порівняйте ефективність аналітичних процесів зі світовими та українськими практиками (бенчмаркінг);
4. Визначити напрямки вдосконалення та розвитку процесу керування доступами.

Для оцінки зрілості процесів ІБ у різних сферах діяльності підприємства я рекомендую використовувати метод оцінки зрілості процесів, розроблений на основі провідних світових практик і стандартів інформаційної безпеки.

2.3.2. Інвентаризація портфеля застосунків

Проведення інвентаризації портфеля застосунків дає можливість зрозуміти які системи містять критичні дані, а які ні, і на основі цього будується стратегія підходу до керування доступами. У світовій практиці застосунки зазвичай класифікують за трьома основними моделями доступу:

- **Стандартні веб-додатки.** Ці програми на основі HTML можуть спілкуватися за допомогою сучасних протоколів ідентифікації, таких як мова розмітки Security Assertion, OpenID та OAuth, як частина повністю федеративного єдиного входу. Багато SaaS-додатків і програмних додатків, які підпадають під цю категорію.
- **Нестандартні веб-додатки.** Ці програми на основі HTML не можуть спілкуватися за допомогою сучасних протоколів ідентифікації, а скоріше вимагають "перекладачів", проксі або агентів, які можуть.
- **Застарілі програми.** Для товстих клієнтських або легких програм доступу до каталогів на основі протоколу або навіть додатків на основі мейнфреймів проксі та агенти обмежені. Кращою стратегією може бути очікування можливого виходу програми на користь стандартного веб-додатка.

Уся зібрана інформація повинна бути зважена на можливості ринку, щоб вибрати правильний інструмент управління доступом і створити дорожню карту інтеграції додатків для об'єктів критичної інфраструктури.

Кожен процес керування доступом оцінюється по п'ятибальній шкалі у відповідності до стану процесу на підприємстві, тлумачення оцінювання процесів наведено у таблиці 2.1.

Таблиця 2.1 – Оцінювання процесів керування доступом у відповідність до їх стану

0	Відсутність жодної базисної спроможності. Незавершений підхід до визначення принципів корпоративного/операційного управління. Може відповідати або не відповідати намірам будь-якої практики процесу.
1	Процес більш менш досягає своїх цілей завдяки застосування незавершеного набору дій, який можна охарактеризувати як початковий або інтуїтивний – не дуже організований.
2	Процес досягає своїх цілей завдяки застосуванню основного, вже повного набору дій, які можуть бути охарактеризовані як виконані.
3	Процес досягає своїх цілей набагато більш організовано з використанням організаційних активів. Процеси, як правило, добре визначені.
4	Процес досягає своїх цілей, чітко визначений та його продуктивність (кількісно) вимірюється.
5	Процес досягає своїх цілей, чітко визначений, його продуктивність вимірюється для підвищення та постійного вдосконалення.

2.3.3. Корпоративне управління

Система корпоративного управління — це сукупність принципів і механізмів, що забезпечують прийняття рішень і контроль за їх виконанням. Аналіз системи корпоративного управління складається з двох етапів:

- аналіз існуючої моделі корпоративного управління;
- аналіз ролі функцій ІБ та відповідності цілям корпоративного бізнесу.

Аналіз існуючої моделі корпоративного управління включає такі етапи:

- Визначити поточний обсяг і цілісність функцій ІБ (процесу керування доступом) для забезпечення захисту критично важливих систем і бізнес-процесів організації;
- Проаналізуйте рівень залучення інших функцій і бізнесів в забезпеченні інформаційної безпеки;
- Перегляньте поточну структуру Керівного комітету та його членів, послідовність і перелік прийнятих рішень у сфері ІБ.

Аналіз ролі функції ІТ та відповідності бізнес-цілям підприємства є важливим для визначення рівня співпраці ІБ з підприємством та запровадити максимальну ефективність від ISMS.

Аналіз ролі ІТ-функції та відповідності цілям корпоративного бізнесу включає наступні етапи:

- Визначте роль, яку відіграє функція ІТ в організації;
- Проаналізувати завдання та повноваження функції ІТ в рамках поточного підпорядкування;
- Проаналізуйте портфель функцій ІТ і цілі, щоб узгодити їх із бізнес-цілями.

2.3.4. Визначення та задоволення потреб у доступі як зовнішніх та і внутрішніх користувачів

Потрібно розглянути випадки використання управління доступом, які розподілені по внутрішніх і зовнішніх округах, включаючи:

- бізнес-співробітник, або управління доступом для робочої сили;
- B2B (бізнес для бізнесу), або управління доступом для постачальників і ділових партнерів;
- B2C (бізнес для споживачів), або управління доступом для клієнтів.

Відсутність єдності щодо того, як збирати, уточнювати та поширювати ідентифікаційні дані, робить механізм IAM з недоліками в роботі та впливає на проект організації з управління доступом. Найкращі світові практики вважають за краще тримати свої圈子 користувачів окремо для об'єктів критичної інфраструктури. Однак це може бути дорожче, це створює кращий поділ за напрямками бізнесу, оскільки кожна спільнота має унікальні вимоги. Окремі каталоги, такі як віртуальні каталоги або метакаталоги, часто використовуються для побудови баз даних ідентифікації. Це дозволяє абстрагуватися від навколишнього середовища, забезпечуючи інструменти управління доступом необхідної інформації для прийняття рішення про доступ, незалежно від типу користувача.

2.3.5. Визначення архітектури ІБ

Інструменти керування доступом пропонують широкий спектр функцій доступу та безпеки. Для того щоб вирішити, яка функціональність потрібна для об'єктів критичної інфраструктури потрібно на ранньому етапі оцінити усі вимоги до практики керування доступом і зверніть пильну увагу на те, як постачальники відповідають цим вимогам.

Наприклад, один постачальник може підтримувати автентифікацію на основі заголовка, тоді як іншому може знадобитися окремий продукт. Один постачальник може підтримувати підхід на основі графічного інтерфейсу до делегованого адміністрування, де інший може надавати лише інтерфейс командного рядка. Оцінка того, як різні постачальники послуг з управління доступом підходять до вимог, допоможе вам вибрати правильний інструмент керування доступом для вашої програми.

Сучасна цифрова трансформація є рушійною силою впровадження IaaS (Інфраструктура як послуга), тоді як впровадження SaaS-додатків для

критичних бізнес-процесів добре демонструється на ринку. Доступність на рівні комунальних послуг тепер є очікуванням для будь-якої пропозиції IAM, що поставляється SaaS, особливо таких важливих послуг, як управління доступом. Деякі постачальники зазнали відключень, залишаючи своїх клієнтів у темряві, коли справа доходить до доступності додатків. Щоб зменшити ризики недоступності або інцидентів безпеки, потрібно вибирати параметри, які забезпечують високу доступність та/або проводять ретельне планування аварійного відновлення та безперервності бізнесу.

2.3.6. Планування та використання суміжної технології IAM (Identity and Access Management)

У суміжній технології IAM можливості багатофакторної аутентифікації (MFA) є основною пропозицією серед інструментів керування доступом, інші можливості менш зрілі. Інструменти керування посвідченнями та адміністрування керують життєвим циклом ідентифікації, відстежують авторизацію та допомагають у підготовці. Більшість інструментів керування доступом не мають зрілих можливостей, тому їх слід доповнювати інструментами управління ідентифікацією та адміністрування. Аналогічно, інструменти керування привілейованим доступом необхідні для відстеження та контролю доступу до облікових записів з розширеним доступом, чого зазвичай не роблять інструменти керування доступом.

У розширенні можливостей безпеки засобів управління доступом важливі компоненти, що додають додаткову вбудовану видимість і контроль. Такі інструменти, як служби безпеки та веб-програми та інструменти захисту API, можуть додавати видимість і елементи керування, які спочатку недоступні в засобах керування доступом.

Коли справа доходить до ІАМ клієнта, віддаленого підтвердження особи та можливостей облікового запису не вистачає серед більшості постачальників керування доступом, як і інструментів для управління згодою та уподобаннями. Додавання цих примикань усуває прогалини в засобах керування доступом.

Керівникам з безпеки та управління ризиками, потрібно обирати більше одного інструменту ІАМ, щоб задовольнити всі вимоги в короткостроковій перспективі.

Висновки до розділу 2

У даному розділі було розглянуто міжнародні стандарти по інформаційних технологіях, які регламентують системний підхід до побудови процесу керування доступом та визначають підхід до побудови системи управління кібербезпекою та державні стандарти, які регламентують процес створення КСЗІ. Також, ми порівняли дані стандарти на їх відповідність до сучасних тенденцій та кіберзагроз.

Було розроблено системний підхід, який дозволяє систематизовано проаналізувати поточний стан організації на відповідність вищесказаним державним та міжнародним стандартам. Також, було описано кожний розділ який входить до побудови ІТ стратегії та які етапи оцінки повинні включати дані розділи. Було описано таблицю, відповідно якої оцінюються початковий стан процесу керування доступом.

РОЗДІЛ 3

СИСТЕМНИЙ ПІДХІД ДО ПРОЦЕСУ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Метою даного розділу є розробка системного підходу до процесу керування доступом в об'єктах критичної інфраструктури в умовах воєнного стану, що може бути застосований при розробці ІТ стратегії. Також в даному розділі буде запропонована високорівнева методика оцінки ризиків.

3.1. Методика оцінки ризиків інформаційної безпеки

Відповідно до вимог міжнародних та національних стандартів інформаційної безпеки одним із основних етапів впровадження системи управління інформаційною безпекою є ідентифікація активів та оцінка ризиків інформаційної безпеки активів. Процес ідентифікації активів дуже популярний і повинен бути запроваджений у будь-якій країні або промислових об'єктах.

Щоб оцінити ризик ідентифікованого активу, ми пропонуємо підхід, який базується на трьох основних моментах:

- сценарій реалізації загрози;
- оцінити ймовірність реалізації загрози;
- оцінити очікувані наслідки впровадження загроз.

3.1.1. Класи активів і типи збитків

Для побудови підходу керування доступом в енергетичному секторі ми рекомендуємо класифікувати всі важливі активи на 3 категорії: технологічна інфраструктура, інфраструктура підприємства та конфіденційні дані.

Технологічна інфраструктура - комплекс активів, сукупність яких забезпечує функціонування технологічних процесів, або розташована в рамках технологічної мережі.

Інфраструктура підприємства – комплекс активів, сукупність яких забезпечує функціональність інфраструктури підприємства або розташована в рамках мережі підприємства.

Конфіденційні дані – інформація, доступ до якої обмежено через її цінність для бізнесу.

3.1.2. Сценарій реалізації загрози

При аналізі можливих сценаріїв реалізації загрози необхідно відповісти на 3 основні питання: «Хто?», «Що?» і «Як?».

3.1.2.1. Хто?

Аналізуючи модель порушника інформаційної безпеки, необхідно зосередитися на зловмисниках, які становлять найбільшу загрозу для бізнесу. У нашому випадку енергетичний сектор перебуває у дуже загрозливому середовищі як об'єкт критичної інфраструктури і у воєнний стан загрозливе середовище лиш збільшується, оскільки для ворога це є мішень номер один.

Енергетична галузь вразлива до численних атак, спрямованих на промислові системи, які контролюють автоматизовані виробничі процеси. Виходячи з історичного досвіду, тенденцій, що виникають, та аналізу загроз енергетичному сектору, основними суб'єктами (злочинцями), які здійснюють загрози, є наступні суб'єкти:

- спонсоровані державою зловмисники – спонсоровані державою хакери або злочинні організації, спрямовані на енергетичний сектор з наміром завдати шкоди критичній інфраструктурі країни:
 - володіють значними внутрішніми ресурсами для підготовки та виконання атак;
 - застосовують складні атаки зі сценаріями, розробленими спеціально для атаки на організацію;
- кіберзлочинці - високомотивовані та добре фінансовані групи, які націлені на енергетичний сектор для отримання фінансової вигоди:
 - використовують атаки, призначені для викрадення конфіденційної інформації та саботажу з метою отримання викупу;
- співробітник із злочинними намірами – працівник або підрядник, чия зловмисна поведінка з метою помсти та фінансової вигоди призводить до порушення інформаційної безпеки:
 - використовують знання про системи та інфраструктуру для диверсій;
 - використовують свою силу для викрадення конфіденційної інформації;
- недбалі працівники - працівники або підрядники, чиї ненавмисні дії призводять до порушення інформаційної безпеки:
 - через атаки соціальної інженерії;
 - через недостатнє знання правил комплаєнсу.
 - через менш ефективний контроль ІБ

- хактивісти — це дуже активні групи активістів, які націлені на корпорації для просування політичних ідей або групу хакерів, щоб отримати визнання:
 - не мають багато ресурсів і часу;
 - використовують атаки на основні вразливості ІБ.

3.1.2.2. Що?

Злочинці мають різні мотиви, які керують їх поведінкою. Знання об'єкта атаки надає контекст про загрози, з якими може зіткнутися бізнес, і можливість зосередитися на впровадженні заходів безпеки інформації.

Основними цілями кібератак є:

- отримати фінансову вигоду від нападу;
- серйозна репутаційна шкода бізнесу;
- вплив на стабільну роботу бізнес-процесів підприємства.

3.1.2.3. Як?

Розуміння методу реалізації загроз під час атаки може допомогти запровадити засоби керування для виявлення та запобігання подібним типам атак у майбутньому. Існує велика кількість способів реалізації загроз. У нашій роботі ми поділяємо ці типи методів на 4 високорівневі категорії:

1. Злом — спроби отримати доступ до інформаційних активів або скомпрометувати їх роботу в обхід механізмів безпеки ІБ (наприклад, використання вразливостей системи, DDoS, грубої сили (bruteforce));
2. Шкідливе програмне забезпечення (ПЗ) - будь-яке шкідливе ПЗ, призначене для зміни стану чи функціональності пристрою без згоди

власника (вірус, бекдор, кейлоггер, шпигунське програмне забезпечення);

3. Соціальна інженерія – соціальне маніпулювання користувачами для використання цільових інформаційних систем або активів (фішингові атаки);
4. Зловживання - навмисне або ненавмисне використання ресурсу/привілеїв неналежним чином (порушення політик)

3.1.2.4. Оцінка ймовірності загрози

Ми рекомендуємо оцінювати ймовірність реалізації ризику на основі інформації про частоту подій, що відбуваються в енергетиці інших суб'єктів господарювання, а також аналізувати інформацію про доступні суб'єктам господарювання методи захисту від певних ризиків. Для оцінки ймовірності будемо використовувати п'ятибальну шкалу оцінок, а саме:

- дуже ймовірно (критично), що ризик реалізується;
- висока ймовірність реалізації ризику;
- середня ймовірність реалізації ризику;
- низька ймовірність реалізації ризику;
- ймовірність реалізації ризику дуже низька.

3.1.2.5. Оцінка очікуваних наслідків від реалізації загрози, а також обробка даних ризиків

У світовій практиці виділяють 4 типи збитків для підприємств: фінансовий, процесний, юридичний, репутаційний.

Фінансовий – результатами даного збитку будуть слугувати фінансові втрати організації, які можуть бути як критичні так і не критичні.

Процесний – результатом даного збитку є порушення функціонування бізнес-процесу підприємства у зв'язку з системними порушеннями.

Юридичний – результат даного збитку пов'язаний з порушеннями відповідностей вимог регулятора, який може призвести до зисків в суді.

Репутаційний – результатом даного збитку є втрата репутації організації серед клієнтів, партнерів, інвесторів та споживачів.

Як результат, під час використання вищенаведеної методики оцінки ризиків є створення профілей ризиків організації, а також плану пониження ризиків ІБ (інформаційна безпека) під час реалізації процесу керування доступом.

3.2. Системний підхід до процесу керування доступом

Для того, щоб уникнути вразливостей процесу керування доступом, а саме процесу автентифікації та подолати вектори загроз потрібно слідувати наступному підходу:

1. Надати високий пріоритет автентифікації без пароля. Паролі та процеси автентифікації на основі паролів страждають від загроз безпеці, таких як фішинг і злом паролів. І підхід автентифікації без пароля є способом усунення цих загроз. Але чому автентифікація на

основі пароля все ще широко реалізована? Відповідь на це, ймовірно, полягає в тому, що автентифікацію на основі пароля легше реалізувати, і рішення "просто працює". Для автентифікації без пароля часто потрібні спеціальні пристрої, і якщо програмне забезпечення опубліковано для ширшої демографічної групи, застосувати автентифікацію без пароля може бути складно, а то й неможливо. Але завдяки зростанню популярності смартфонів із функціями Touch ID і Face ID, а також доступності апаратних маркерів безпеки, таких як U2F-ключі та специфікацій, як-от WebAuthn, які легко носити з собою, зараз ідеальний час для пріоритету автентифікації без пароля.

2. Впровадити федеративний вхід і єдиний вхід (SSO). Система єдиного входу (SSO) дозволяє користувачам входити в кілька програм за допомогою одного набору облікових даних. І федеративний вхід дозволяє користувачам автентифікуватися за допомогою ідентифікаційних даних, підтверджених третьою стороною (наприклад, увійти за допомогою Google, увійти за допомогою Facebook). Якщо ваша програмна програма не є постачальником ідентифікаційної інформації, немає сенсу впроваджувати процес перевірки особи. Стандарти автентифікації, такі як OAuth2, OpenID Connect і SAML, значно спрощують реалізацію федеративного входу та SSO. Важливим застереженням під час використання федеративної автентифікації та SSO є правильна реалізація процесу обміну автентичності. Хоча ці стандарти безпечні за своєю схемою, безпека залежить від реалізації. Як і в будь-якому програмному забезпеченні, уразливості в реалізації протоколу є поширеними. Найкраще використовувати протоколи SAML і OAuth2.
3. Посилена функція автентифікації. Посилення функціональності автентифікації є важливою частиною правильного впровадження

потоків автентифікації. Нижче наведено шість найкращих методів, які допоможуть уникнути логічних помилок і захистити функцію автентифікації.

- a. Безпечний процес відновлення облікового запису. Незахищений процес відновлення облікового запису можна використати для обходу процесу автентифікації. Нижче наведено кілька важливих функцій, які слід враховувати під час розробки процесу відновлення облікового запису:
 - i. Процес відновлення облікового запису має бути захищений за допомогою другого етапу автентифікації;
 - ii. Згенеруйте криптографічно захищене випадкове значення для маркерів скидання;
 - iii. Переконайтеся, що маркери скидання надсилаються через HTTPS;
 - iv. Термін дії токенів скидається під час першого використання та забезпечує короткий час життя (TTL);
 - v. Повторно автентифікуйте користувачів для оновлення пароля, навіть якщо вони вже перебувають у сеансі автентифікації;
 - vi. Захистіть процес відновлення облікового запису від атак CSRF (Атаки на підробку міжсайтових запитів);
- b. Безпечне керування сеансами. Оскільки сеанси зберігають автентифікований стан користувачів, порушення процесу керування сеансом дозволяє зловмисним користувачам обійти процес автентифікації або видати себе за інших користувачів. Нижче наведено кілька важливих функцій, які слід враховувати під час впровадження процесу керування сеансом:
 - i. Використовуйте криптографічно безпечні випадкові значення для файлів cookie сеансу;

- ii. Сеансом завжди слід керувати на стороні сервера;
 - iii. Застосуйте атрибути безпеки файлів cookie, зокрема Secure, HttpOnly, SameSite, Domain, Path, Expire та Max-Age;
 - iv. Обережно зберігайте дані сеансу в localStorage і sessionStorage;
 - v. Переконайтеся, що маркери сеансу генеруються заново під час кожного нового входу та знищуються після виходу користувача;
 - vi. Реалізуйте тайм-аут неактивного сеансу;
- c. Використовуйте безпечні та перевірені бібліотеки автентифікації та відстежуйте наявність вразливостей у залежностях. Безпека бібліотек, які використовуються як залежні для побудови функцій автентифікації, також є важливим фактором, який слід враховувати. Наприклад, уразливість, яка дозволяла зловмиснику повністю обійти перевірку XML-підпису та видати змінений файл за підписаний за допомогою ретельно створеного XML-файлу, була виявлена в бібліотеці Go XML Digital Signature. Ця бібліотека використовується багатьма популярними програмами на основі Go для автентифікації SAML. Це вплинуло навіть на Teleport, що було виправлено у випуску 4.1.11. Використовуйте засоби сканування вразливостей залежностей, такі як аудит npm, дотримуйтеся порад CVE, пов'язаних із мовою програмування (наприклад, .net CVE, python CVE), і дотримуйтесь проактивних методів постійного моніторингу вразливостей залежностей.
- d. Створюйте елементи керування, щоб запобігати логічним помилкам і утримувати їх. Логічні недоліки важко виявити, і

вони можуть мати серйозні наслідки. Належний дизайн програмного забезпечення з оглядом інженерів безпеки є першим кроком, щоб уникнути логічних недоліків безпеки. Крім того, розробники програмного забезпечення повинні бути навчені щодо поширених уразливостей, пов'язаних із процесом автентифікації, і навчені запобігати цим уразливостям. Серія шпаргалок автентифікації від OWASP — чудове місце, щоб дізнатися, як безпечно реалізувати функцію автентифікації.

е. Реалізація двофакторної автентифікації (2FA). Двофакторна автентифікація, ймовірно, найкращий спосіб покращити безпеку процесу автентифікації. Можна з упевненістю сказати, що правильно реалізований метод 2FA може допомогти вам запобігти серйозній уразливості в процесі автентифікації. Але навіть процес 2FA може бути вразливим і його можна обійти, якщо його реалізовано ненадійно. Нижче наведено кілька способів посилити впровадження 2FA:

- i. Віддавайте перевагу 2FA без пароля/без PIN-коду (наприклад, U2F), а не 2FA на основі пароля/PIN-коду (TOTP, SMS);
- ii. Переконайтеся, що автентифіковані сеанси створюються лише з дійсним станом перевірки 2FA, який зберігається на сервері;
- iii. Виконайте повторну автентифікацію, щоб оновити налаштування 2FA;
- iv. Запровадити обмеження швидкості в невдалому 2FA;
- v. 2FA захищає від скомпрометованих облікових даних і уповільнює або запобігає автоматизованим атакам. Тому переконайтеся, що 2FA застосовується за замовчуванням у кожному процесі автентифікації.

- f. Запровадити взаємну автентифікацію. Взаємна автентифікація передбачає автентифікацію обох підключених сторін (клієнта та сервера) і найкраще підходить для автентифікації API та міжмашинної автентифікації. Взаємна автентифікація також зазвичай використовується як додатковий фактор довіри, окрім облікових даних, таких як паролі. Взаємну автентифікацію можна реалізувати за допомогою сертифікатів та інфраструктури відкритих ключів (PKI). Такі протоколи, як SSH і TLS, мають вбудовану підтримку взаємної автентифікації.
4. Захист від автоматизованих атак. Впровадити обмежувачі швидкості. Впровадження обмежувачів швидкості допомагає зупинити атаки грубої сили. Простий обмежувач швидкості, який зараховує невдалі спроби автентифікації та блокує користувачів на певний період, може значно підвищити безпеку та зупинити атаки грубої сили. Для служб на основі API, які зазвичай обробляють великий обсяг запитів автентифікації, алгоритми сегментів маркерів і блоків з витоком є популярними алгоритмами для впровадження обмежувачів швидкості. Також рекомендовано додати CAPTCHA. CAPTCHA – чудовий спосіб уповільнити автоматизовані атаки. Хоча справжнім користувачам часто неприємно розгадувати CAPTCHA, його можна використовувати разом із обмежувачами швидкості, щоб CAPTCHA запитували лише ті користувачі чи машини, які порушують правила обмеження швидкості.
5. Посилити автентифікацію на основі пароля. Хоча загальна порада полягає в тому, щоб надавати перевагу безпарольному рішенню, у багатьох випадках це нелегка міграція. Нижче наведено кілька рекомендацій щодо захисту автентифікації на основі пароля.

- a. Застосуйте надійну ентропію пароля. Засоби перевірки надійності пароля, такі як `zxcvbn`, можуть бути корисними для реалізації сильної ентропії;
 - b. Не надсилайте програмне забезпечення у виробництво з паролями за замовчуванням;
 - c. Не встановлюйте паролі `root`. Натомість створіть логіку автентифікації, яка вимагає від користувачів самотійно встановлювати паролі під час першого входу. Наприклад, під час налаштування облікового запису згенеруйте короточасний маркер, який можна обміняти для встановлення паролів. Для порівняння Teleport використовує подібний метод обміну маркерами для налаштування облікового запису користувача;
 - d. Заборонити використання відомих паролів. Це можна реалізувати шляхом перехресної перевірки за допомогою публічних списків паролів, таких як загальні облікові дані SecList, або за допомогою таких служб, як `haveibeenpwned`;
 - e. Хешуйте паролі перед збереженням у базі даних за допомогою безпечних алгоритмів хешування паролів, таких як `Argon2`, `scrypt` або `bcrypt`. Щоб ще більше підвищити безпеку, додайте сіль і перець до хеш-значень;
6. Не винаходьте заново методи автентифікації. Легко написати функцію автентифікації, але важче правильно реалізувати. Бібліотеки, сертифіковані стандартними специфікаціями (наприклад, сертифіковані OpenID Connect) і перевірені на безпеку бібліотеки є безпечнішим вибором. Може виникнути спокуса винайти власні протоколи автентифікації та використовувати спеціальні криптографічні алгоритми для захисту процесу автентифікації, але це може бути дуже ризиковано, тому не рекомендується.

Найкращі рекомендації для захисту процесу автентифікації – це пріоритет автентифікації без пароля та впровадження федеративного входу або SSO із двофакторною автентифікацією. Міркування про безпеку необхідно враховувати на ранніх стадіях процесу проектування, щоб реалізувати елементи керування, які запобігають логічним помилкам. Регулярні аудити безпеки також важливі для перевірки на наявність логічних недоліків, і слід ретельно обмірковувати вибір бібліотек і залежностей для процесу автентифікації.

3.3. Тест – приклад, який демонструє авторизацію в систему

Під час розробки системного підходу до процесу керування доступом, а саме процесу аутентифікації та авторизації було також розроблено пілотний проект, який демонструє всі етапи добре налаштованого процесу аутентифікації, який забезпечує безпеку інформаційним системам критичної інфраструктури енергетичного сектору в умовах воєнного стану. Оскільки саме у воєнний стан багато кібератак загрожують енергетичному сектору, для того щоб зруйнувати всю систему із середини. Застосування кібератак є зручною зброєю, оскільки їх можна виконувати анонімно та з будь-якої точки світу.

Отже, ефективний приклад аутентифікації складається з наступних етапів, які також продемонстровані в рисунках на тест прикладі:

1. Проводимо налаштування SAML із допомогою Auth0 протоколу. Автентифікація єдиного входу SAML зазвичай включає постачальника послуг та постачальника ідентифікаційних даних. Процес потоку зазвичай включає етапи встановлення довіри та процесу аутентифікації. Нашим постачальником ідентифікаційних даних є Auth0, а постачальник послуг – вигадана послуга, EnergoSave.

2. Тепер користувач намагається отримати доступ до EnergoSave за допомогою аутентифікації SAML (рис. 3.1).

```
<saml2p:AuthRequest ID="3438545343948990fed276ddfg" IssueInstant = "2022-10-28T13:12:51.133TV" AssertionConsumerServiceURL = "https://energосave.com/saml" Version = "2.0">
<saml2:Issuer>https://energосave.com</saml2:Issuer>
</saml2p:AuthnRequest>
```

Рисунок 3.1 - Користувач намагається увійти в EnergoSave з браузера.
EnergoSave відповідає, генеруючи запит SAML.

3. Браузер перенаправляє користувача на URL-адресу SSO, Auth0. Auth0 аналізує запит SAML і автентифікує користувача. Це може бути з іменем користувача та паролем або навіть із входом у соціальні мережі. Якщо користувач вже пройшов автентифікацію на Auth0, цей крок буде пропущено. Після автентифікації користувача Auth0 генерує відповідь SAML (рис.3.2).

```
<saml2p:Response ID="6789933c5h87dd201ke54wa2g" InResponseTo="3438545343948990fed276ddfg" IssueInstant="2016-10-30T13:13:28.153TZ" Version="2.0">
<saml2:Issuer>https://auth.idp.com</saml2:Issuer>
<saml2p:Status>
  <saml2p:StatusCode />
</saml2p:Status>
<saml2p:Assertion ID="a48fg332dw98h786kc5c6y7s4n" IssueInstant="2016-10-30T13:13:28.151TZ" Version="2.0">
  <saml2:Issuer>https://auth.idp.com</saml2:Issuer>
  <ds:Signature></ds:Signature>
  <saml2:Subject>
    <saml2:NameID>Prosper@zagadat.com</saml2:NameID>
    <saml2:SubjectConfirmation>
      <saml2:SubjectConfirmationData InResponseTo="3438545343948990fed276ddfg" NotOnOrAfter="2016-10-30T13:13:28.153TZ" Recipient="https://zagadat.com" />
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2016-10-30T13:13:28.151TZ" NotOnOrAfter="2016-10-30T13:13:28.152TZ">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://zagadat.com</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ" SessionIndex="32413b2e54db89c764fb96ya2k" SessionNotOnOrAfter="2016-10-30T13:13:28.152TZ">
    <saml2:SubjectLocality />
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="e-mail">
      <saml2:AttributeValue xsi:type="xs:anyType">Prosper@zagadata.com</saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2p:Assertion>
</saml2p:Response>
```

Рисунок 3.2 - Auth0 аналізує запит SAML і автентифікує користувача.

4. Auth0 повертає закодовану відповідь SAML браузеру. Браузер відправляє відповідь SAML в EnergoSave для перевірки. Якщо перевірка буде успішною, користувач увійде в EnergoSave і отримає доступ до ресурсів, які він має право переглядати/змінювати (рис. 3.3).

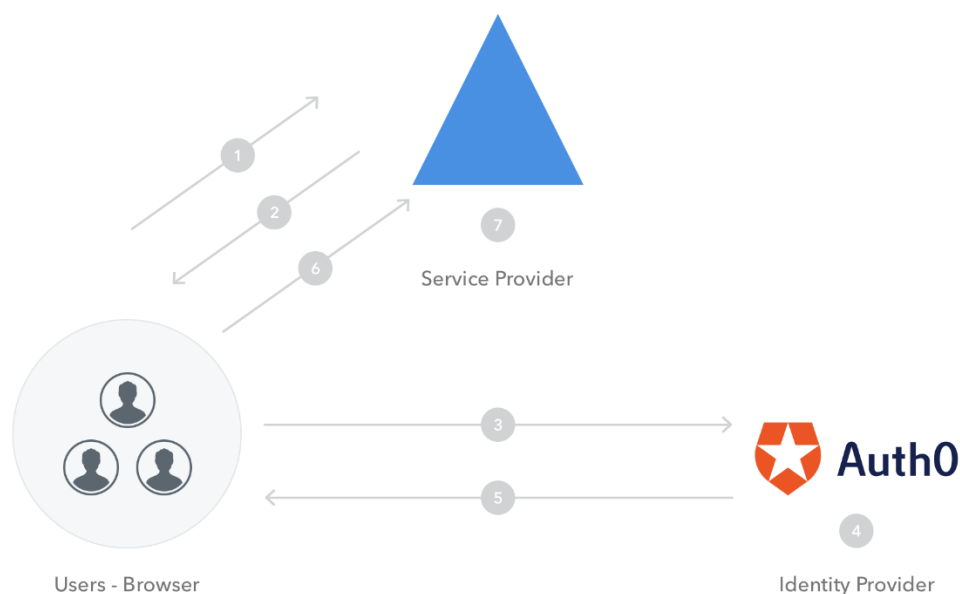


Рисунок 3.3 - Схема технологічного процесу.

Також, розглянемо як це буде відображатися в самій системі, в графічному інтерфейсі, використовуючи SSO та двохфакторну аутентифікацію:

1. Заходимо на сторінку аутентифікації (рис. 3.4) та вводимо SSO ID

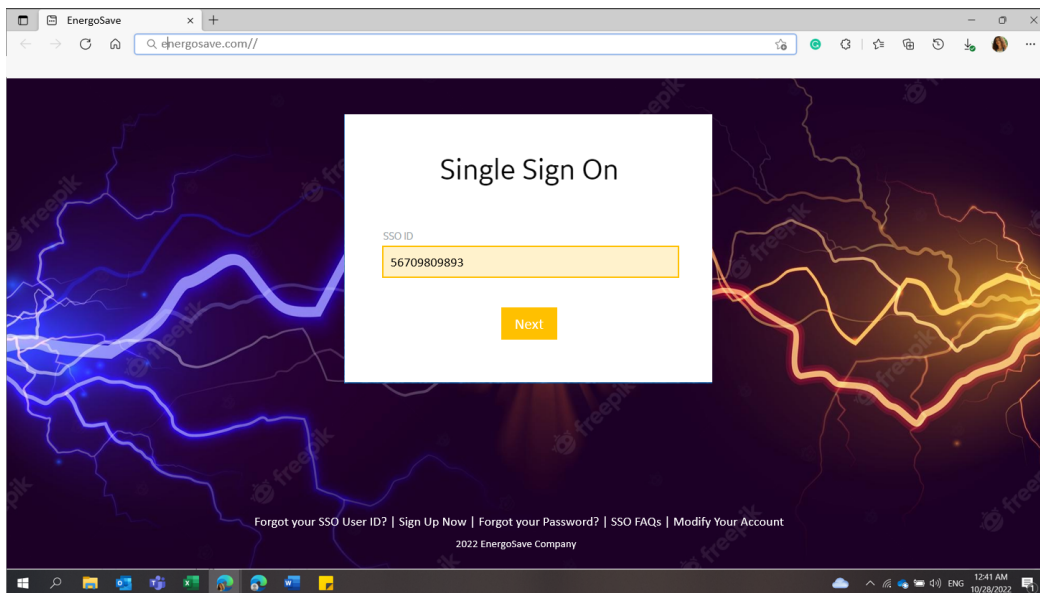


Рисунок 3.4 - Сторінка входу (SSO).

2. Вводимо пароль (рис. 3.5)

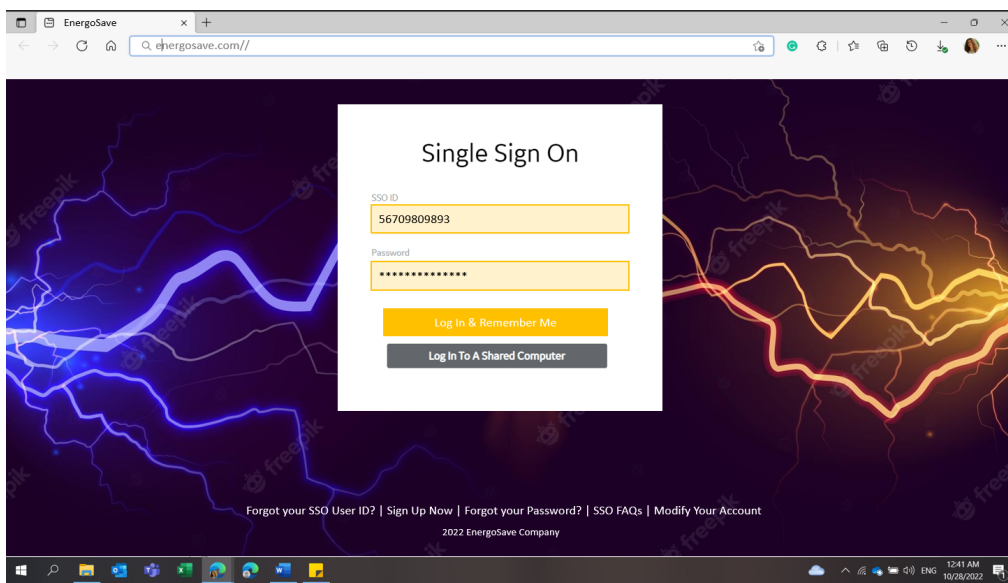


Рисунок 3.5 - Процес аутентифікації.

3. Використання двофакторної авторизації (рис. 3.6, рис. 3.7)

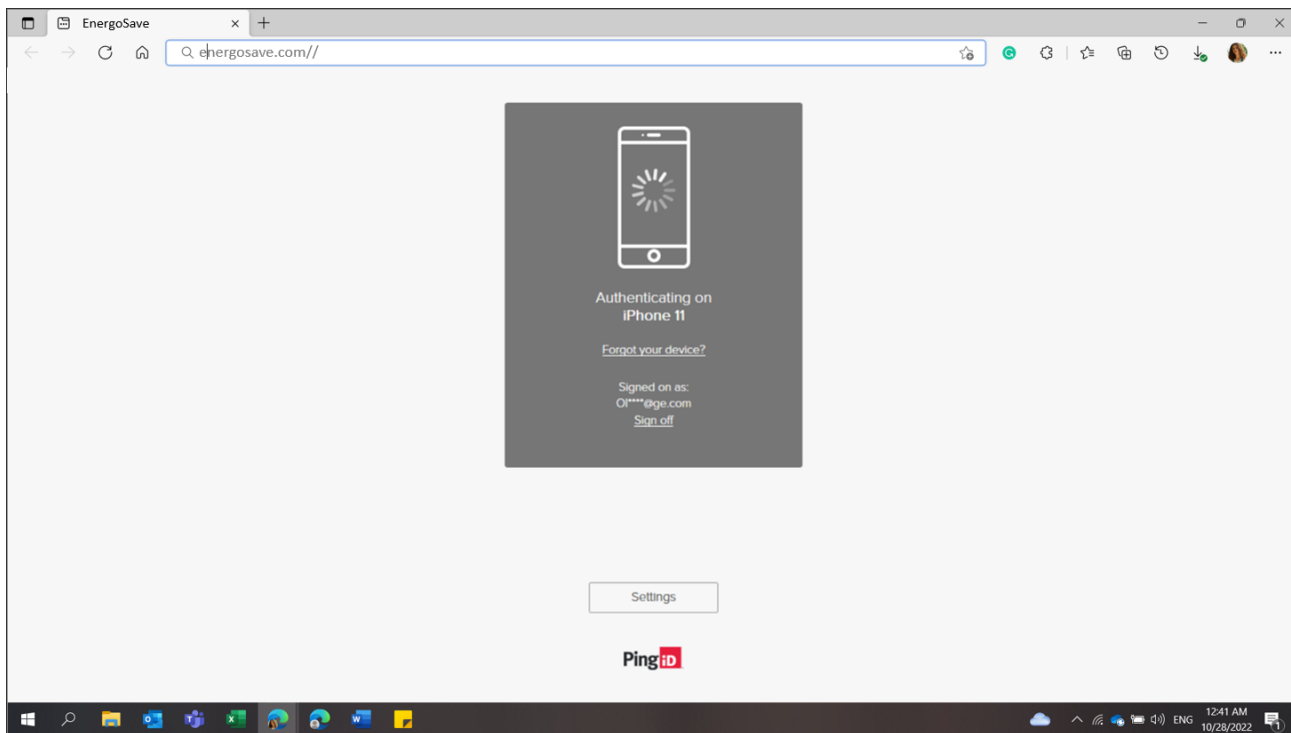


Рисунок 3.6 - Використання двохфакторної аутентифікації.

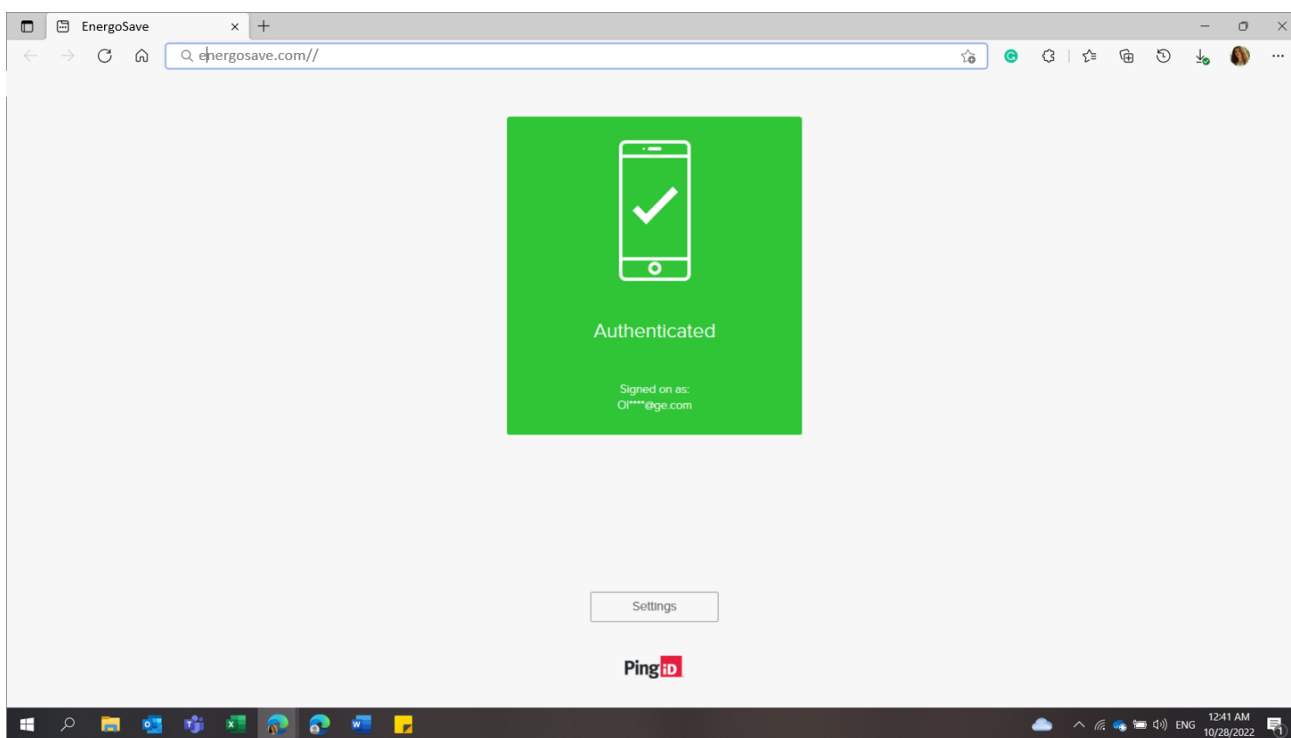


Рисунок 3.7 - Успішний вхід.

Висновки до розділу 3

У цьому розділі було розроблено методику оцінки ризиків, а також розроблено системний підхід до процесу керування доступом у відповідності з контролями та кращими практиками для технічних засобів забезпечення інформаційної безпеки для об'єктів критичної інфраструктури в умовах воєнного стану.

Як результат, також було розроблено тестовий приклад ефективної та безпечної аутентифікації, оскільки на сам перед все залежить від аутентифікації, хто може зайти в систему і чи немає процес аутентифікації вразливих місць.

РОЗДІЛ 4

РОЗРОБКА ВЛАСНОГО СТАРТАП ПРОЕКТУ

Розділ має на меті проведення маркетингового аналізу стартап проекту задля визначення принципової можливості його ринкового впровадження та можливих напрямів реалізації цього впровадження. Зараз у сучасному світі існує велика потреба в забезпеченні надійного процесу керування доступом для забезпечення цілісності, конфіденційності та доступності інформації. Взагалі є багато систем які використовують класичні методи такі як паролі, які в даний час є взагалі не надійними.

Все це означає, що проблема, яку вирішує стартап, являється актуальною і може стати успішним на ринку та стати основним вибором для переважної кількості цільової аудиторії.

4.1. План розробки стартапу та масштабування його на ринок

Наведемо план розробки стартапу та виведення його на ринок. Спочатку треба провести маркетинговий аналіз, який включає в себе:

- конкурентний аналіз, щоб зрозуміти, якими методами вирішення проблем вже користуються люди;
- формування ідеї самого проекту та виділення цільової аудиторії;
- розробити стратегію виведення товару на ринок, базуючись на аналізі ринкового середовища.

Наступним кроком являється організація самого стартапу. На цьому етапі мають бути:

- складений весь план та побудований таймлайн розробки та запуску продукту;

- запланований обсяг виробництва та оцінений потенційний обсяг ресурсу, який буде потрібен для виконання плану;
- розраховані витрати, необхідні для реалізації проекту, та витрати на запуск проекту.

Далі необхідно виконати фінансово-економічний аналіз та оцінити ризики стартап-проекту, в межах якого:

- визначити обсяг інвестиційних витрат;
- розрахувати основні фінансово-економічні показники проекту (собівартість, ціну продукту/послуги, податковий збір та чистий прибуток) та визначити показники інвестиційної привабливості проекту (рентабельність продажів, період окупності проекту);
- визначити основні ризики проекту та способи для їх запобігання.

Фінальним кроком являється розробка заходів з комерціалізації продукту. Цей крок являється важливим для масштабування та збільшення розмірів продукту.

Для того, щоб залучити інвесторів та знайти різні способи фінансування проекту, необхідно:

- провести дослідження на предмет інтересів потенційних інвесторів та бізнесів;
- скласти інвестиційну пропозицію, яка включає в себе як опис самого продукту та його теперішні розміри, так і можливі шляхи розширення та розвитку;
- обрати канали комунікації із потенційно зацікавленими персонами.

Далі наведемо результати виконання кожного з описаних кроків.

4.2. Опис ідеї стартап-проекту

Стартап-проект полягає у вирішенні проблеми забезпечення конфіденційності, цілісності та доступності інформації в енергетичному секторі. Суть продукту стартапу полягає у тому, щоб розробити системний підхід до захисту даних в енергетичному секторі критичної інфраструктури.

У таблиці 4.1 наведена інформаційна карта стартапу.

Таблиця 4.1 – Інформаційна карта стартап-проекту.

Назва проекту	Energosave
Автори проекту	Пастушок Олена Олегівна
Коротка анотація	Надати бізнесу та спеціалістам з інформаційної безпеки якісний інструмент для оцінки зрілості стану процесів керування доступом сумісно з відповідністю вимогам стандарту ITIL.
Термін реалізації проекту	12 місяців
Необхідні ресурси	Приміщення з комп'ютерами, доступом до Інтернету, доступ до електромережі Програмне забезпечення для розробки, хмарне сховище для даних, антивірусні програми Фінансові кошти на оплату заробітної плати виконавцям на термін 12 місяців, а також на такі витрати як: оренда приміщення, комунальні послуги, оренда хмарного сховища тощо

Продовження таблиці 4.1.

Опис проблеми, яку вирішує проект	Продукт вирішує задачу збереження цілісності, конфіденційності та доступності інформації
Головні цілі та завдання проекту	Метою проекту є надати бізнесу та спеціалістам з інформаційної безпеки якісний інструмент для оцінки зрілості стану процесів керування доступом
Очікувані результати	Привернення організацій з критичною інфраструктурою до нашого стартапу, створення нового підходу

4.3 Технологічний аудит ідеї проекту

Тепер можна розібрати ідею стартапу та провести конкурентний аналіз. У таблиці 4.2 наведений опис ідеї стартапу.

Таблиця 4.2 – Опис ідеї стартапу.

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Надати бізнесу та спеціалістам з інформаційної безпеки якісний інструмент для оцінки зрілості стану процесів керування доступом сумісно з відповідністю вимогам стандарту ITIL.	1. Оцінка зрілості процесів ІБ	1. Легкість в використанні
	2. Оцінка зрілості технічної архітектури ІБ	2. Комплексний підхід до оцінки

Продовження таблиці 4.2.

	3. Виконання вимоги постійного вдосконалення СУІБ згідно стандарту	3. Відповідність доменам стандарту ITIL, можливість одночасної оцінки
--	--	---

Далі проведемо порівняльний аналіз конкурентів проекту та наведемо результати у таблиці 4.3.

Таблиця 4.3 – Порівняльний аналіз конкурентів проекту.

№ п/п	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	ITIL	COBIT 2019	CISO			
1.	Зручність	5	4	3	2	-	-	+
2.	Простота	5	2	2	3	-	-	+
3.	Повнота	5	4	4	3	-	-	+
4.	Сумісність	5	3	3	2	-	-	+

Далі аналізуємо реальність технічно здійснити ідею проекту (таблиця 4.4).

Таблиця 4.4 – Технологічна здійсненність продукту.

№ п/п	Ідея проекту	Технології і реалізації	Наявність технологій	Доступність технологій
1	Надати бізнесу та спеціалістам з інформаційної безпеки якісний інструмент для оцінки зрілості стану процесів	Використання протоколів SAML та Auth0	Наявні	Доступні
2	керування доступом сумісно з відповідністю вимогам стандарту ITIL.	Використання шифрування даних	Не наявні, необхідні допрацювання	Доступні
3		Використання шифрування сховища ключів	Наявні, необхідні допрацювання	Доступні
Обрана технологія реалізації ідеї проекту: SAML, Auth0				

4.4. Аналіз ринкових можливостей запуску стартап-проекту

Далі проведемо попередній аналіз ринку для запуску стартап-проекту (таблиця 4.5).

Таблиця 4.5 – Попередня характеристика потенційного ринку стартап-проекту.

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	13
2	Загальний обсяг продаж, грн/ум.од	4000
3	Динаміка ринку (якісна оцінка)	Зростає

Продовження таблиці 4.5.

4	Наявність обмежень для входу (вказати характер обмежень)	Професійна репутація
5	Специфічні вимоги до стандартизації та сертифікації	Необхідно сертифікувати модель згідно з вимогами стандартизованої організації ITIL
6	Середня норма рентабельності в галузі (або по ринку), %	75

Тепер проведемо характеристику потенційних клієнтів, які можуть бути зацікавлені в проекті (таблиця 4.6).

Таблиця 4.6 – Характеристика потенційних клієнтів стартап-проекту.

№ п/п	Потреби, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Потреба в відповідності вимогам стандарту ITIL в частині постійного вдосконалення та оцінка зрілості стану процесу керування доступом на підприємстві	Бізнес, який йде на сертифікацію СУІБ та з бізнес-середовищем високого ризику з точки зору ІБ, який вимагає високої зрілості процесів керування доступом	Одні клієнти можуть вибирати модель з точки зору ефективної для оцінки зрілості, а інші – для виконання вимоги постійного вдосконалення СУІБ	- продукт повинен давати чітку інструкцію до використання - компанія повинна пройти сертифікацію на відповідність вимогам ISO

Обрахуємо фактори загроз (таблиця 4.7) та можливостей (таблиця 4.8). Проаналізуємо загрози, щоб зрозуміти можливі перешкоди при запуску продукт на ринок. Фактори можливостей же треба обрахувати, щоб знати усі сприятливі умови та по можливості ними скористатися.

Таблиця 4.7 – Фактори загроз.

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Конкуренція	Хоча ринок є відкритим і неосвоїним, на ньому вже є кілька великих гравців, які відомі на ринку, які вже мають свою цільову групу покупців	Знайти точки додаткової цінності для користувача
2	Ціна збуту	Конкуренти можуть коштувати менше через нижчу якість	Сфокусуватися на якості роботи застосунку та продумати маркетингову стратегію
3	Якість аналізу	Через комплексність задачі, потрібно регулярно оновлювати рекомендації, оскільки кібератаки щороку стають все більш новіші та небезпечніші	Мати достатній штаб і ресурси, для аналізу сучасних проблем та швидкого оновлення

Таблиця 4.8 – Фактори можливостей.

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Універсальність	Продукт не залежить від апаратної платформи як у більшості конкурентів	Зробити акцент при маркетингу, продовжувати розвиток як окремого продукту
2	Простота у використанні	Від користувача треба лише дотримуватися підходу	Реалізувати зручний інтерфейс для вивчення
3	Якість та гарантії	Надавати найбільш якісні послуги та сервіси	Відповідність міжнародним стандартам

Далі розглянемо питання конкуренції, а саме визначимо її тип та рівень (таблиця 4.9).

Таблиця 4.9 – Ступеневий аналіз конкуренції на ринку.

Особливості конкурентного середовища	У чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Вказати тип конкуренції: недосконала конкуренція	Представлено мало хороших методологій та експертів	Зробити максимальним збут застосунку

Продовження таблиці 4.9.

2. За рівнем конкурентної боротьби: міжнародний	Наявні проекти, розроблені та можуть бути доступні у всьому світі	Розширити цільову аудиторію, розробити підхід на різних мовах
3. За галузевою ознакою: внутрішньогалузева	Можуть працювати з різними галузями	Покращити персоналізацію
4. Конкуренція за видами товарів: товарно-родова	Конкуренція з аналізами інших систем та експертів	Підтримувати та покращувати якість існуючих функцій
5. За характером конкурентних переваг: нецінова	Різні компанії пропонують різну якість	Розробляти якісніші алгоритми і моделі
6. За інтенсивністю: марочна	Вже представлені компанії із сильним брендом	Предметно створити комунікаційну стратегію для вибудови свого бренду

Далі необхідно виконаємо аналіз конкуренції за моделлю 5 сил конкуренції Майкла Портера (таблиця 4.10).

Таблиця 4.10 – Аналіз конкуренції в галузі за М. Портером.

Складові аналізу	Прямі конкуренти у галузі	Потенційні конкуренти	Постачальники	Клієнти	Товарозамінники
	Інші існуючі методології та продукти	Якість, ціни, кількість користувачів, капіталовкладення	Фактори сили постачальників	Контроль якості, порівняння цін	Сила бренду, якість, ціна, масштаби
Висновки	Конкуренція з невеликою інтенсивністю, а також підігрітий ринок	Можливості входження на ринок, нові потенційні конкуренти	Постачальники відсутні	Клієнти не диктують умови роботи на ринку	Товарозамінники відсутні

Маючи результати аналізу конкуренції (таблиця 4.10), характеристики ідеї стартап-проекту (таблиця 4.5), характеристики потенційних клієнтів і їх вимоги до продукту (таблиця 4.6) та фактори ринкового середовища (таблиці 4.7 і 4.8) було сформульовано та обґрунтовано перелік факторів конкурентоспроможності (таблиця 4.11).

Таблиця 4.11 – Обґрунтування факторів конкурентоспроможності.

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Універсальність	Продукт не залежить від апаратної платформи як у більшості конкурентів
2	Простота у використанні	Від користувача треба лише дотримуватися підходу
3	Якість та гарантії	Надавати найбільш якісні послуги та сервіси

Тепер можна провести аналіз сильних та слабких сторін продукту (таблиця 4.12).

Таблиця 4.12 – Порівняльний аналіз сильних та слабких сторін системи.

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів						
			-3	-2	-1	0	1	2	3
1	Універсальність	20	+						
2	Простота у використанні	16		+					
3	Якість та гарантії	10		+					

Далі проведемо SWOT-аналіз продукту (таблиця 4.13).

Таблиця 4.13 – SWOT-аналіз стартап-проекту.

Сильні сторони Універсальність Простота у використанні Якість та гарантії	Слабкі сторони Відсутність сильного бренду Не сформована база клієнтів Не підключені альтернативні канали маркетингу
Можливості Покращення системи Персоналізація	Загрози Нові системи та експерти Збут

Дякуючи проведенню SWOT-аналізу, ми змогли визначити сильні та слабкі сторони, можливості та загрози, пов'язані з конкуренцією та плануванням стартап-проекту. Далі спроектуємо альтернативну ринкову поведінку для інтеграції стартап-проекту на ринок та приблизний час реалізації системного комплексу, з урахуванням потенційних проектів, що можуть бути виведені на ринок та наведемо результати у таблиці 4.14.

Таблиця 4.14 – Альтернативи ринкового впровадження стартап проекту.

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Вихід на ринок з нижче якістю	70%	4 місяці
2	Пропонувати одразу платне використання	50%	6 місяців
3	Представлення користувачам системи без інтерфейсу	60%	5 місяці

У даному пункті був проведений детальний аналіз ринку та продукту. Також відповідно до результатів проведеного конкурентного аналізу, визначених факторів ринку та його сприятливості, описання ідеї та характеристик стартап-проекту, робимо висновок, що існують дуже сприятливі умови для виходу продукту на ринок.

4.5. Розроблення ринкової стратегії стартап-проекту

Для розробки ринкової стратегії продукту, у першу чергу, необхідно проаналізувати цільову аудиторію проекту (таблиця 4.15).

Таблиця 4.15 – Вибір цільових груп потенційних споживачів.

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит у межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Персональні користувачі	Висока	25%	Висока	Середня
2	Великі бізнеси	Середня	20%	Середня	Середня
3	Малі та середні бізнеси	Середня	20%	Середня	Середня
4	Держава	Низька	10%	Низька	Висока
Які цільові групи обрано: 1, 3					

Маючи аналіз цільових груп, далі визначимо базову стратегію розвитку продукту (таблиця 4.16).

Таблиця 4.16 – Визначення базової стратегії розвитку.

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	1 та 3	Диференційованого маркетингу	Масштабування та максимізація	Оптимальних витрат

Для роботи в обраних сегментах ринку сформовано базову стратегію розвитку (таблиці 4.17, 4.18).

Таблиця 4.17 – Визначення базової стратегії конкурентної поведінки.

Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
Ні	Так	Ні	Виклику лідера

Таблиця 4.18 – Визначення стратегії позиціонування.

Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспро- можні позиції власного стартап- проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
Універсальність Простота у використанні Якість результатів	Оптимальних витрат	Універсальність Простота у використанні Якість та гарантії	Система, яка краще всіх забезпечує цілісність, конфіденційність та доступність інформації

4.6. Розроблення маркетингової програми стартап-проекту

Після проведеного комплексного аналізу, можемо повноцінно описати ключові переваги концепції потенційного товару (таблиця 4.19) та побудувати концепцію маркетингових комунікацій (таблиця 4.20).

Таблиця 4.19 – Ключові переваги концепції потенційного товару.

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Якісна генерація	Збереження конфіденційних даних	Постійне покращення методики, які зможуть вберегти від сучасних кібератак
2	Універсальність	Методологія не залежить від апаратної платформи	Такого виду системний підхід може використовувати будь- який користувач
3	Простий інтерфейс	Системний підхід дуже простий у використанні	Системний підхід із інтуїтивно зрозумілими пунктами для збереження конфіденційності, доступності та цілісності інформації

Таблиця 4.20 – Концепція маркетингових комунікацій.

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Пошук спеціалізованих систем	b2b продажі Зв'язок через теплі контакти Таргетована реклама у соціальних мережах Публікація в спеціалізованих виданнях, журналах	Точність Якість Універсальність	Поєднати повідомлення про те, що це якісна методолгія яка є незалежною	Таргетована реклама на цільову аудиторію
2	Пошук доступного та дешевого продукту	Рекламні банери в Інтернеті, форуми, реклами від інфлюенсерів	Простота	Вселити довіру у бренд та продукт	Реклама у лідерів думок Вивіски в публічних місцях Таргетована реклама на цільову аудиторію

Висновки до розділу 4

Даний розділ був присвячений дослідженню стартап-проекту. В якості такого був представлений системний підхід для збереження конфіденційності, доступності та цілісності інформації.

У рамках розділу було досліджено розробку стратегій виходу на ринок та маркетинг-стратегії для цього. Зокрема, даний ринок являється сприятливим з невеликою кількістю представлених компаній конкурентів. Оскільки вони дають лише частину функцій, а запропонована система є універсальною та доступною, то у стартап-проекту є всі шанси стати монополістами на ринку.

Також були опрацьовані сильні та слабкі сторони проекту, SWOT аналіз, аналіз конкурентів та цільової аудиторії. На основі всіх досліджень був сформований концепт маркетингової стратегії для обраних цільових аудиторій.

ВИСНОВКИ

Дана робота присвячена вивченню та аналізу вимог державних та міжнародних стандартів інформаційної безпеки та їх застосовності до об'єктів критичної інфраструктури в умовах воєнного стану.

У роботі розглянуто актуальне визначення об'єктів критичної інфраструктури на рівні законодавства, проаналізовано вимоги, що висуваються до даних об'єктів. Розглянуто закон про «Стратегії інформаційної безпеки України» та проаналізовано його застосовність для розробки стратегії інформаційної безпеки підприємств. Проведено порівняльний аналіз державних та міжнародних стандартів інформаційної безпеки.

Запропоновано системний підхід до процесу керування доступом в об'єктах критичної інфраструктури в енергетичному секторі в умовах воєнного стану, а також було розглянуто етапи аналізу кожної складової системного підходу. Розроблено методику оцінки ризиків та на її основі продемонстровано реалізацію профілю ризиків та приклад оцінки та обробки ризиків. На основі визначених ризиків та контролів, було розроблено системний підхід до процесу керування доступом з детальним обґрунтуванням кожного з технічних рішень використаних у цій моделі.

В результаті розроблені методики та моделі було об'єднано в підхід впровадження технічних рішень інформаційної безпеки на підприємстві, що є однією з основних складових стратегії інформаційної безпеки. Розроблене рішення є унікальне тим, що надає практичні для застосування методики з оцінки актуального стану ІТ та ІБ архітектури та процесів підприємства, демонструє приклади класифікації ризиків, збитків та активів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Закон України про критичну інфраструктуру URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 20 вересня 2022 року).
2. Об'єкти критичної інфраструктури URL: https://uk.wikipedia.org/wiki/Об%27єкти_критичної_інфраструктури (дата звернення: 20 вересня 2022 року).
3. Вірус Petya URL: <https://www.trellix.com/en-us/security-awareness/ransomware/petya.html> (дата звернення: 20 вересня 2022 року).
4. Енергетика України під час воєнного стану. Зміни у вимогах URL: https://jURL:iga.ligazakon.net/ru/aktualno/12602_energetika-vo-vremya-voyny-v-ukraine-kakie-izmeneniya-v-regulirovanii (дата звернення: 20 вересня 2022 року).
5. Постанова про покладення спеціальних обов'язків на учасників ринку електричної енергії, що здійснюють операції з експорту електричної енергії, для забезпечення загальносупільних інтересів у процесі функціонування ринку електричної енергії протягом дії воєнного стану URL: https://ips.ligazakon.net/document/view/KP220775?bl=&_ga=2.68433938.2031580460.1663787590-746212929.1663787590 (дата звернення: 20 вересня 2022 року).
6. ЗАКОН УКРАЇНИ Про внесення змін до деяких законів України щодо розвитку установок зберігання енергії URL: https://ips.ligazakon.net/document/view/T222046?bl=&_ga=2.102445058.2031580460.1663787590-746212929.1663787590 (дата звернення: 20 вересня 2022 року).

7. Постанова про затвердження Ліцензійних умов провадження господарської діяльності зі зберігання енергії URL: https://ips.ligazakon.net/document/view/GK51828?_ga=2.102445058.2031580460.1663787590-746212929.1663787590 (дата звернення: 20 вересня 2022 року).
8. Проект закону України про особливості регулювання відносин на ринку природного газу та у сфері теплопостачання під час дії воєнного стану та подальшого відновлення їх функціонування URL: https://ips.ligazakon.net/document/view/ji07502i?_ga=2.181100452.2031580460.1663787590-746212929.1663787590 (дата звернення: 20 вересня 2022 року).
9. Наказ про заборону експорту природного газу URL: https://ips.ligazakon.net/document/view/FN073512?bl=&_ga=2.173244192.2031580460.1663787590-746212929.1663787590 (дата звернення: 20 вересня 2022 року).
10. Why cyberattacks happen URL: <https://www.ibm.com/topics/cyber-attack> (дата звернення: 20 вересня 2022 року).
11. Вірус WannaCry URL: <https://www.malwarebytes.com/wannacry> (дата звернення: 20 вересня 2022 року).
12. Вірус Stuxnet URL: <https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html> (дата звернення: 20 вересня 2022 року).
13. Ukraine's power outage was a cyber attack: Ukrenergо URL: <https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA> (дата звернення: 20 вересня 2022 року).
14. What is access control? URL: <https://www.citrix.com/solutions/secure-access/what-is-access-control.html> (дата звернення: 20 вересня 2022 року).
15. ДСТУ 2155-93 Енергозбереження. Методи визначення економічної ефективності заходів по енергозбереженню (2155-93) URL:

- <https://budinfo.org.ua/doc/1812280/DSTU-2155-93-Energozberezhennia-Metodi-viznachennia-ekonomichnoi-efektivnosti-zakhodiv-po-energozberezhenniu> (дата звернення: 20 вересня 2022 року).
16. ДСТУ ISO/IEC 27001:2015. Технічний комітет зі стандартизації «Інформаційні технології». — 2015. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910 (дата звернення: 20 вересня 2022 року).
17. ITIL Access Management: Objectives, Process And Values URL: <https://www.invensislearning.com/blog/itil-access-management/> (дата звернення: 20 вересня 2022 року).
18. What is IT Strategy? URL: <https://thinkinsights.net/digital/it-strategy/#What-is-IT-Strategy> (дата звернення: 20 вересня 2022 року).

ДОДАТОК А

ПРЕЗЕНТАЦІЯ



Рисунок А.1 – Початок презентації.

Основна інформація


ОБ'ЄКТ ДОСЛІДЖЕННЯ
Об'єктом дослідження є стратегія керування доступом в об'єктах критичної інфраструктури


ПРЕДМЕТ ДОСЛІДЖЕННЯ
Предметом дослідження є державні та міжнародні стандарти з інформаційної безпеки, а також методики розробки стратегій керування доступом


МЕТА КВАЛІФІКАЦІЙНОЇ МАГІСТЕРСЬКОЇ РОБОТИ
Мета кваліфікаційної магістерської роботи – визначення застосованих державних стандартів до об'єктів критичної інфраструктури, порівняння державних та міжнародних стандартів ІБ, розробка систематичного підходу до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану


ПРАКТИЧНА ЗНАЧУЩІСТЬ ОТРИМАНИХ РЕЗУЛЬТАТІВ
Практичне значення отриманих результатів полягає у розробці системного підходу, методики оцінки стану підприємства та розробки тестового прикладу, який демонструє надійний захист, що забезпечує конфіденційність, цілісність та доступність інформації критичної інфраструктури.



12/10/22
Prepared by Olena Pastushok
2

Рисунок А.2 – Основна інформація.

Основна інформація

ОСНОВНІ ЗАВДАННЯ

- Огляд актуальних державних стандартів з інформаційної безпеки (ІБ)
- Порівняння державних стандартів з сучасними міжнародними стандартами ІТ
- Визначення об'єктів критичної інфраструктури у відповідності до законодавства України
- Опис методології розробки системного підходу до процесу керування доступами
- Розробка методики оцінки ІТ ризиків
- Розробка системного підходу до процесу керування доступами

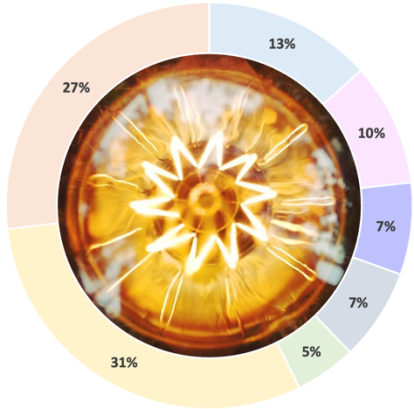
НАУКОВА НОВИЗНА РОБОТИ

Наукова новизна роботи полягає в розробці системного підходу до процесу керування доступом в об'єктах критичної інфраструктури в умовах воєнного стану, що поєднує в собі найкращі практики міжнародних стандартів та виконання вимог державних стандартів

12/10/22 Prepared by Olena Pastushok 3

Рисунок А.3 – Основна інформація.

Актуальність магістерської роботи



Сектор	Відсоток
Уряд та місцеві органи влади	13%
Фінансовий сектор	10%
Телеком та програмне забезпечення	7%
Інше	7%
Сектор безпеки та оборони	5%
Комерційний сектор	31%
Енергетика	27%

Загалом протягом **15–22 березня** Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала **70 кібератак**

За **останні 6 років** у світі в **57 разів** збільшилась кількість кібератак на об'єкти критичної інфраструктури

За даними Держспецзв'язку, з **24 лютого** відбулося **825 атак** на сайти в Україні

Інтенсивність нападів залишається високою протягом усієї війни — так, за **II квартал** було здійснено **548 спроб** злому ресурсів

12/10/22 Prepared by Olena Pastushok 4

Рисунок А.4 – Актуальність магістерської роботи.

Об'єкти критичної інфраструктури

Космічні технології та послуги	Виготовлення вакцин та функціонування біолабораторій	Енергозабезпечення	Водопостачання
Хімічна промисловість	Охорона здоров'я	Надання адміністративних послуг та урядування	Водовідведення
Інформаційні послуги	Служби порятунку та цивільний захист населення та територій	Фармацевтична промисловість	Постачання теплої енергії
Продовольче забезпечення	Електронні комунікації	Транспортне забезпечення	Тримання під вартою, правопорядок та здійснення правосуддя
Дослідницька діяльність	Фінансові послуги	Державна безпека та оборона	Космічна діяльність

12/10/22

Prepared by Olena Pastushok

5

Рисунок А.5 – Об'єкти критичної інфраструктури.

Процес управління доступом відповідно державних та міжнародних стандартів



12/10/22

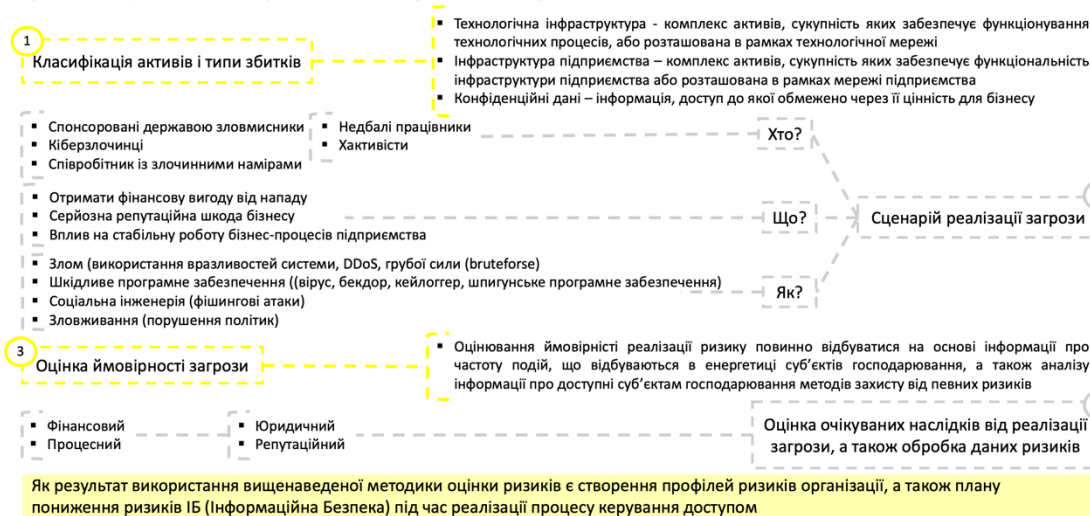
Prepared by Olena Pastushok

6

Рисунок А.6 – Процес управління доступом відповідно державних та міжнародних стандартів.

Методика оцінки ризиків інформаційної безпеки

Методика оцінки ризиків інформаційної безпеки базується на трьох елементах: сценарій реалізації загрози, оцінка ймовірності реалізації загрози, оцінка очікуваних наслідків впровадження загрози



12/10/22

Prepared by Olena Pastushok

Рисунок А.7 – Методика оцінки ризиків інформаційної безпеки.

Системний підхід до процесу керування доступом

- Надати високий пріоритет автентифікації без пароля**
Паролі та процеси автентифікації на основі паролів страждають від загроз безпеці, таких як фішинг і злом паролів. І підхід автентифікації без пароля є способом усунення цих загроз
- Впровадити федеративний і єдиний вхід (SSO)**
Система єдиного входу (SSO) дозволяє користувачам входити в кілька програм за допомогою одного набору облікових даних. І федеративний вхід дозволяє користувачам автентифікуватися за допомогою ідентифікаційних даних, підтверджених третьою стороною
- Посилена функція автентифікації**
Безпечний процес відновлення облікового запису, безпечне керування сеансами, використання безпечних та перевірених бібліотек автентифікації та відстежування наявних вразливостей, створення елементів керування для запобігання логічних помилок та утримування їх, реалізація двофакторної автентифікації, запровадження взаємної автентифікації
- Захист від автоматизованих атак**
Впровадження обмежувачів швидкості. Впровадження обмежувачів швидкості допомагає зупинити атаки грубої сили
- Посилити автентифікацію на основі пароля**
Застосуйте надійну ентропію пароля, не надсилайте програмне забезпечення у виробництво з пароллями за замовчуванням, не встановлюйте паролі goot, забороніть використання відомих паролів, хешуйте паролі перед збереженням у базі даних
- Не винаходьте заново методи автентифікації**
Бібліотеки, сертифіковані стандартними специфікаціями (наприклад, сертифіковані OpenID Connect) і перевірені на безпеку бібліотеки є безпечнішим вибором

12/10/22

Prepared by Olena Pastushok

Рисунок А.8 – Системний підхід до процесу керування доступом.

Налаштування SAML із допомогою Auth0 протоколу



12/10/22

Prepared by Olena Pastushok

9

Рисунок А.9 – Налаштування SAML із допомогою Auth0 протоколу.

Графічний приклад, який демонструє реалізацію надійного метода аутентифікації (1/2)

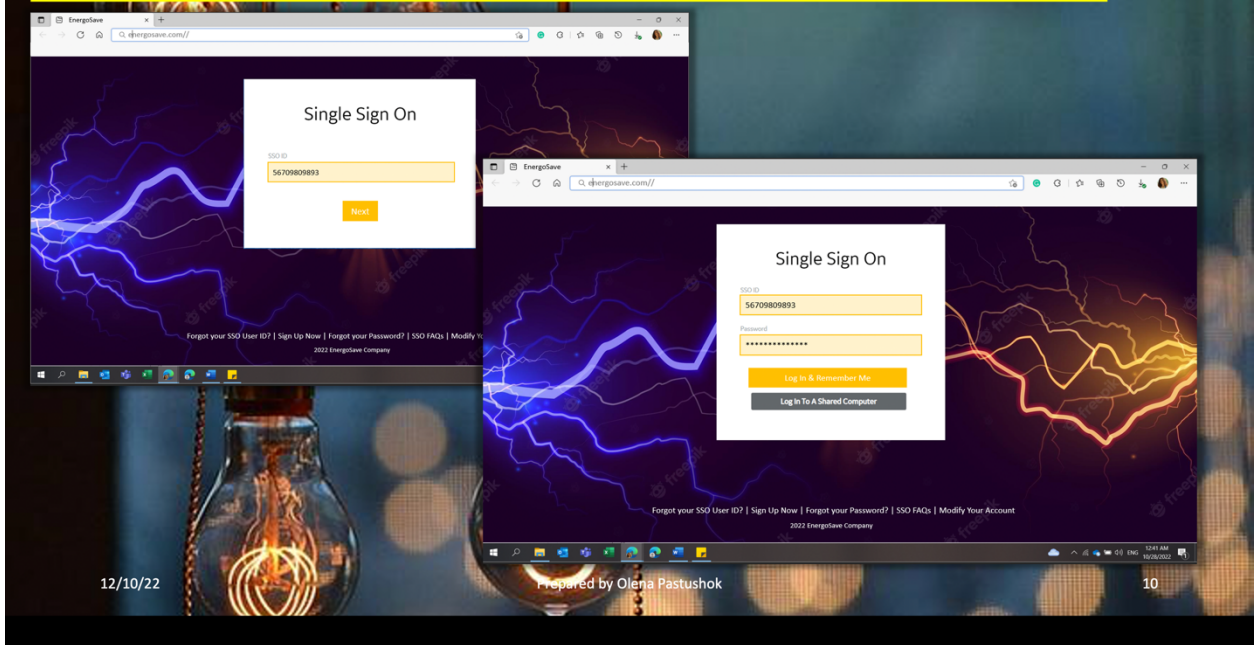


Рисунок А.10 – Графічний приклад, який демонструє реалізацію надійного метода аутентифікації (1/2).

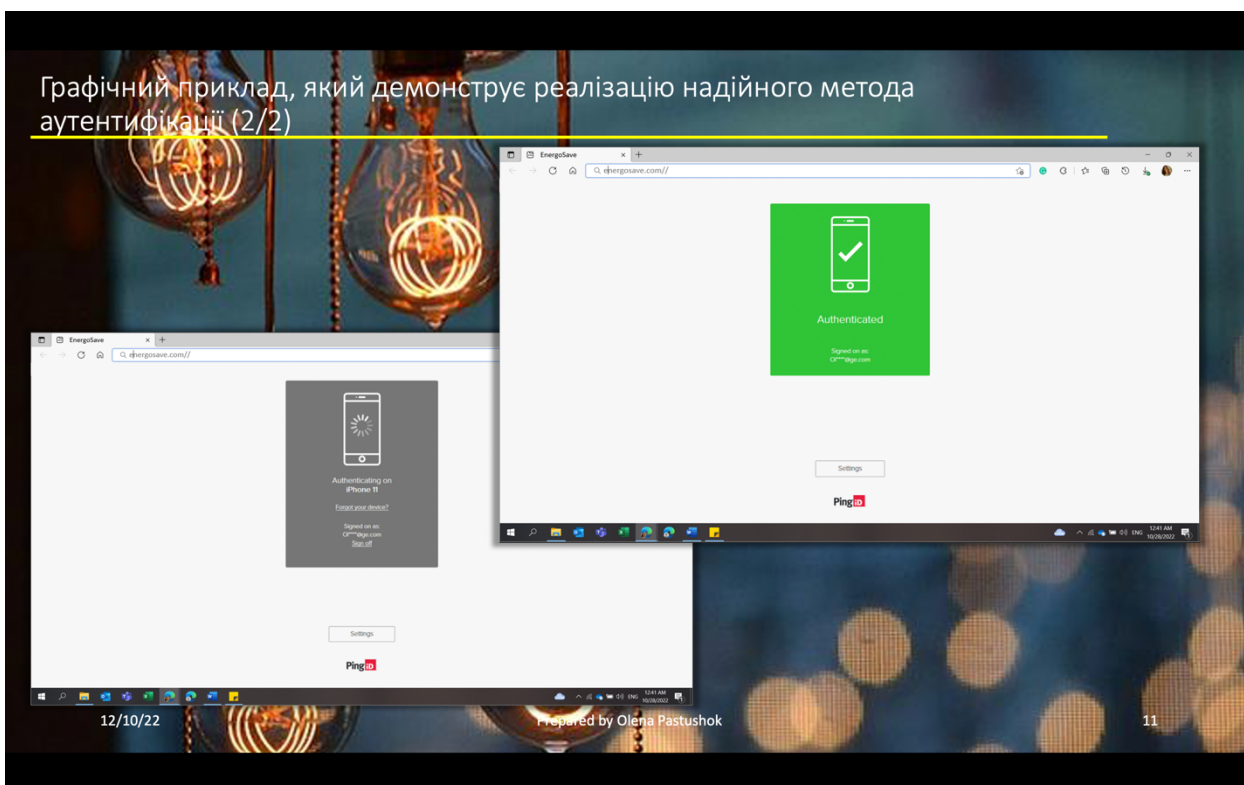


Рисунок А.11 – Графічний приклад, який демонструє реалізацію надійного метода аутентифікації (2/2).

Публікації

1. Тимошук О. Л., Пастушок О. О. Системний підхід до процесу керування доступами в об'єктах критичної інфраструктури в умовах воєнного стану. *Методи забезпечення конфіденційності, цілісності та доступності інформації*: матеріали І науково-практичної конференції «Системні науки та інформатика», 22-29 листопада 2022 року, Київ. – К., НН ІПСА КПІ ім. Ігоря Сікорського, 2022. – ст. 78-81.

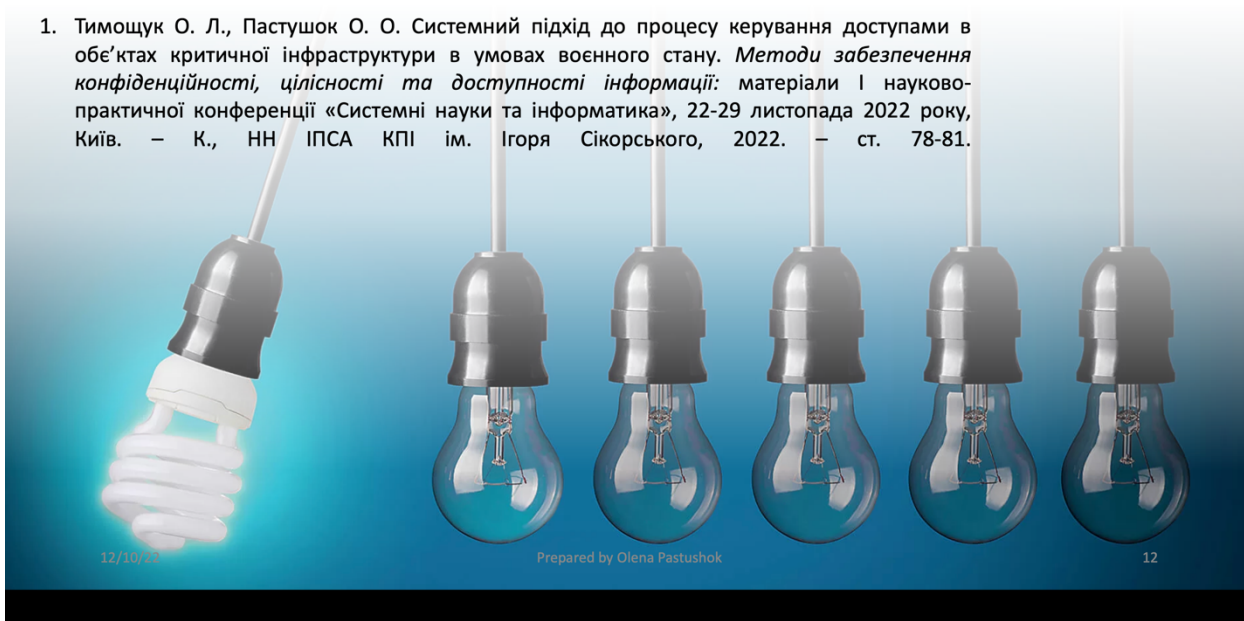


Рисунок А.12 – Публікації.

Висновки



12/10/22

Prepared by Olena Pastushok

13



Рисунок А.13 – Висновки.

Наступні кроки дослідження



12/10/22

Prepared by Olena Pastushok

14



Рисунок А.14 – Наступні кроки дослідження.

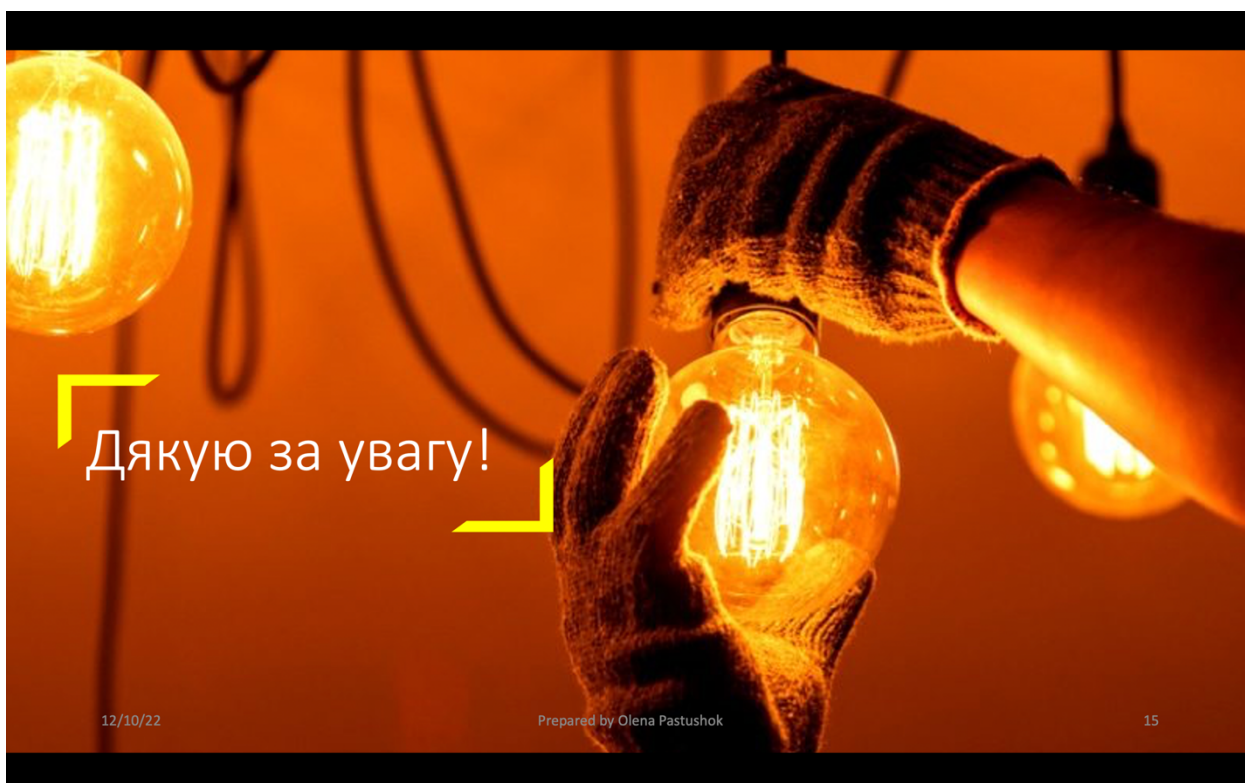


Рисунок А.15 – Завершальний слайд.

ДОДАТОК Б

ЛІСТИНГ ПРОГРАМИ

POST /sap/bc/sec/oauth2/token HTTP/1.1

Authorization: Basic ...=

Content-Type: application/x-www-form-urlencoded;charset=UTF-8

Host: host.example.com:443

Content-Length: 3947

Connection: Keep-Alive

client_id=OA2_TEST&scope=OAUTH2_TEST_SCOPE1&grant_type=urn:ietf:params:oauth:grant-type:saml2-bearer&assertion=PEFzc2VydGlvbiBJ....

<Assertion ID="_ba59ce78-478a-4e81-ba59-4e8cb6ec4644" IssueInstant="2022-10-04T12:03:21.852Z" Version="2.0"

xmlns="urn:oasis:names:tc:SAML:2.0:assertion">

<Issuer>TEST_CLIENT</Issuer>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:SignedInfo>

<ds:CanonicalizationMethod

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

<ds:SignatureMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />

<ds:Reference URI="#_ba59ce78-478a-4e81-ba59-4e8cb6ec4644">

<ds:Transforms>

<ds:Transform

Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />

<ds:Transform

Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />

```

        </ds:Transforms>
        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>

<ds:DigestValue>a+W4gwTA3TsjFu/4Ay3q2T9tcuQ=</ds:DigestValue>
        </ds:Reference>
        </ds:SignedInfo>
<ds:SignatureValue>sfg0LT2Pb2kFD9lW5WKCC8bbhTflj3YHWvF5HcM5jFT0
ZW7aI0KKfjT9QQqytd7UkCKNwU1LX++eeCeWTyhTJjDzmPNiygpLrHZ024C
nTw9Qtrn8skjdOYeL6HLLI5fRAmBerDclaa0/qTck0OnlX5MRzeI1qYty/htIX/w
LegA=</ds:SignatureValue>
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmlsig#">
                <X509Data>
                        <X509Certificate>...=</X509Certificate>
                </X509Data>
        </KeyInfo>
</ds:Signature>
<Subject>
        <NameID>SOKOLOVA</NameID>
        <SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <SubjectConfirmationData NotOnOrAfter="2022-10-
04T1220:03:21.868Z"
Recipient="https://host.example.com:44345/sap/bc/sec/oauth2/token"/>
        </SubjectConfirmation>
</Subject>
<Conditions>
        <AudienceRestriction>
                <Audience>OAT_000</Audience>

```

```
        </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2022-10-04T12:03:21.870Z">
        <AuthnContext>
            <AuthnContextClassRef>urn:none</AuthnContextClassRef>
        </AuthnContext>
    </AuthnStatement>
</Assertion>
```