

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки**

В.о. завідувача кафедри

До захисту допущено

_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)

«_____» _____ 2021 р.

Дипломна робота

на здобуття ступеня бакалавра

**за освітньо-професійною програмою «Системи, технології та
математичні методи кібербезпеки»
спеціальності: 125 «Кібербезпека»**

на тему: створення КСЗІ у комунальному підприємстві України

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-74

(шифр групи)

Сорбот Володимир Олексійович
(прізвище, ім'я, по батькові) _____ (підпис)

Керівник доктор технічних наук, професор Даник Юрій Григорович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) _____ (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) _____ (підпис)

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без
відповідних посилань.
Здобувач вищої освіти _____

(підпис)

Київ - 2021 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 125 «Кібербезпека»

Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)

«__» _____ 2021 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Сорбота Володимира Олексійовича

(прізвище, ім'я, по батькові)

1. Тема роботи: “Створення КСЗІ у комунальному підприємстві України” , керівник роботи Даник Юрій Григорович, професор кафедри інформаційної безпеки ФТІ, затверджені наказом по університету від « _____ » _____ 2021 р. № _____

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи існуючі готові продукти КСЗІ, існуючі методи та етапи створення КСЗІ, існуюча СЗІ на комунальному підприємстві.

4. Зміст роботи

ВСТУП

Існуючі комплексні системи захисту інформації

Етапи створення КСЗІ на даному підприємстві

Розробка КСЗІ у комунальному підприємстві

Висновки

Дата видачі завдання «12» квітня 2021 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми дипломного проекту, визначення мети та постановка задач.	13.04.21-20.04.21	виконано
2	Узгодження теми з дипломним керівником.	21.04.21-23.04.21	виконано
3	Визначення структури дипломного проекту.	24.04.12-29.04.21	виконано
4	Робота над першим розділом: огляд існуючих КСЗІ, дослідження СЗІ на підприємстві, виявлення недоліків та загроз	30.04.21-07.04.21	виконано
5	Робота над другим розділом: модифікація етапів створення КСЗІ з орієнтацією на комунальне підприємство	09.04.21-15.04.21	виконано
6	Робота над третім розділом: аудит безпеки комунального підприємства, розробка моделі загроз, рішення та пропозиції щодо покращення системи захисту інформації.	16.04.21-23.04.21	виконано
7	Попередній розгляд дипломного проекту на кафедрі		

Здобувач вищої освіти

(підпис)

Сорбот В.О

(Власне ім'я, ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Даник Ю.Г.

(Власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Робота складається з 69 сторінок, містить 11 рисунків, 5 таблиць, 1 формулу та 12 літературних посилань.

Метою дипломної роботи є аналіз і дослідження існуючої системи захисту інформації, включаючи технічні та програмні засоби захисту інформації та розробка пропозицій щодо її покращення відносно існуючої системи захисту інформації задля підвищення рівня безпеки підприємства.

Об'єктом дослідження є процес захисту інформації у КП “Київський метрополітен” та його недоліки.

Предмет дослідження: методи, методики, моделі і інструменти створення КСЗІ для захисту інформації.

Методи дослідження. Бібліосемантичний, аналізу, синтезу, моделювання.

Наукова новизна отриманих результатів полягає в проведенні аналізу КСЗІ для підприємства та розробці її удосконаленої версії на основі впровадження запропоновано доповнення до вже існуючої СЗІ на підприємстві, що покращує захищеність інформації на даному об'єкті.

Практичне значення одержаних результатів полягає в здійсненні удосконалення на основі впровадження запропонованого доповнення до вже існуючої СЗІ на підприємстві, що покращує захищеність інформації на даному об'єкті.

Результатом даної роботи було виявлення існуючих проблем у безпеці інформаційних ресурсів на комунальному підприємстві та запропоновані методи їх знешкодження.

Статтю з оглядом існуючих проблем та їх причин було опубліковано у матеріалах Всеукраїнської науково-практичної конференції “Фізико-технічні аспекти кібербезпеки”, 13-14 травня 2021 року.

Ключові слова: *КСЗІ, СЗІ, технічні, програмні, засоби захисту інформації, безпека, інформація, проблеми, ризики, загрози*

ABSTRACT

The work consists of 69 pages, 11 pictures, 5 tables, 1 equation and 12 citations.

The purpose of this work is to investigate the existing system of information protection, including technical and program methods of protection and to offer an upgrade to the existing system of information protection to improve the safety of a communal union.

The subject of research is the existing system of information protection in the CU “Kyivskiy metropoliten” and its disadvantages.

Research methods include analysis of existing methods of building a complex information security system of government information protection, their steps and documentation that must be created during each step, detection and investigation of existing risks and threats to the security of the information in this communal union.

The result of this work was the detection of existing problems in the security of information resources in the communal union and the offering of methods of their disposal.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів.....	9
Вступ.....	10
1 Аналіз існуючих комплексних систем захисту інформації.....	12
1.1 Огляд існуючих комплексних систем захисту інформації.....	12
1.2 Недоліки СЗІ на даному комунальному підприємстві.....	31
Висновки до розділу 1.....	34
2 Етапи створення КСЗІ на підприємстві КП “Київський метрополітен”.....	35
2.1 Обстеження середовищ функціонування ІТС.....	35
2.2 Розробка політики безпеки інформації в ІТС.....	39
2.3 Розробка технічного завдання на створення КСЗІ.....	39
2.4 Розробка проекту КСЗІ.....	40
2.5 Підготовка КСЗІ до введення в дію.....	44
2.6 Навчання користувачів.....	44
2.7 Попередні випробування.....	44
2.8 Дослідна експлуатація.....	46
2.9 Державна експертиза КСЗІ.....	46
2.10 Супроводження КСЗІ.....	47
Висновки до розділу 2.....	47
3 Розробка удосконаленої КСЗІ для комунального підприємства “Київський метрополітен”.....	49
3.1 Аудит інформаційної безпеки комунального підприємства.....	49
3.2 Вимоги до створення КСЗІ.....	57
3.3 Програмно-апаратний захист комунального підприємства.....	58
3.4 Фізичний захист інформації.....	63
3.5 Організаційний захист інформації.....	65
Висновки щодо розділу 3.....	66
Висновки.....	68

Перелік джерел посилання.....	69
-------------------------------	----

ПЕРЕЛІК УМОВИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ

І ТЕРМІНІВ

КСЗІ - комплексна система захисту інформації;

СУІБ - система управління інформаційною безпекою;

ОС - операційна система;

ПЕОМ - персональна електронно-обчислювальна машина;

ЕОМ - електронно-обчислювальна машина;

ПЗ - програмне забезпечення;

НСД - несанкціонований доступ;

ІзОД - інформація з обмеженим доступом;

ПАК - програмно-апаратний комплекс;

БД - база даних;

НДМ - недекларовані можливості;

ВІ - віртуальна інфраструктура;

СБ - сервер безпеки;

ІТС - інформаційно-телекомунікаційна система;

КЗЗ - комплекс засобів захисту від несанкціонованого доступу;

КС - комп'ютерна система;

НД - нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НДР - науково-дослідна робота;

ОТЗ - основні технічні засоби;

ПЕМВН - побічні електромагнітні випромінювання та наведення;

СЗІ - служба захисту інформації;

ТЗ - технічне завдання;

ТЗІ - технічний захист інформації.

ВСТУП

Актуальність роботи: Ухвалення рішень у всіх сферах життєдіяльності підприємства або організації все більшою мірою базується на інформаційних процесах. аналіз цих процесів з наступним виробленням керуючих рішень здійснюється на основі інформаційних моделей, побудованих на сучасних інформаційно-телекомунікаційних технологіях. Тому захист інформації являє собою самостійну складову безпеки підприємства в цілому, значення якої з кожним роком зростає.

Інформаційний ресурс стає одним з головних джерел економічної ефективності підприємства. Фактично спостерігається тенденція, коли все сфери життєдіяльності підприємства стають залежними від інформаційного розвитку, в процесі якого вони самі породжують інформацію і самі ж її споживають.

Звідси і потреба як в створенні комплексної системи захисту інформації (КСЗІ) на підприємстві, так і в проведенні випробувань і оцінки її ефективності, підготовці фахівців з даного профілю.

Метою дослідження є аналіз і дослідження існуючої системи захисту інформації, включаючи технічні та програмні засоби захисту інформації та розробка пропозицій щодо її покращення відносно існуючої системи захисту інформації задля підвищення рівня безпеки підприємства.

Завдання дослідження:

1. Проаналізувати існуючі засоби створення КСЗІ, області інформації, яку вони захищають;
2. Розробити методику створення КСЗІ на підприємстві, що було розглянуто;
3. Запропонувати покращення СЗІ на даному підприємстві, вказавши на існуючі недоліки та запропонувавши засоби зниження ймовірності атаки.

Об'єктом дослідження є процес захисту інформації у КП “Київський метрополітен” та її недоліки.

Предмет дослідження: методи, методики, моделі і інструменти створення КСЗІ для захисту інформації.

Методи дослідження. Бібліосемантичний, аналізу, синтезу, моделювання.

Наукова новизна отриманих результатів полягає в проведенні аналізу КСЗІ для підприємства та розробці її удосконаленої версії на основі впровадження запропоновано доповнення до вже існуючої СЗІ на підприємстві, що покращує захищеність інформації на даному об'єкті.

Практичне значення одержаних результатів полягає в здійсненні удосконалення на основі впровадження запропонованого доповнення до вже існуючої СЗІ на підприємстві, що покращує захищеність інформації на даному об'єкті.

Статтю з оглядом існуючих проблем та їх причин було опубліковано у матеріалах Всеукраїнської науково-практичної конференції “Фізико-технічні аспекти кібербезпеки”, 13-14 травня 2021 року.

1 АНАЛІЗ ІСНУЮЧИХ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Огляд існуючих комплексних систем захисту інформації

Наразі більшість компаній відмовляється від комплексних систем в угоду СУІБ, оскільки отримати атестат відповідності ISO/IEC 27001 набагато простіше, не кажуче вже про те, що для його отримання не обов'язково реалізовувати всі технології захисту одразу, достатньо лише дати обіцянку реалізувати їх до кінця року. Складність побудови КСЗІ обумовлюється також тим, що вона потребує розміщення деякої інфраструктури на території України. Ця вимога, у свою чергу, не є “зручною” для деяких компаній, отже, вони заохочені у відміні стандарту КСЗІ та переходу на СУІБ.

У даній роботі досліджуватимуться існуючі комплексні системи захисту інформації. Оскільки існує багато готових СЗІ, роздивимось 3 (три) з них.

1.1.1 КСЗІ “Панцир+”

Розроблена компанією ООО “НПП “ІТБ” КСЗІ “Панцир+”[1] являє собою СЗІ класу “Last Frontier”. Основна мета цієї СЗІ не виявлення кіберзагроз на початкових стадіях їх зародження, що може бути ефективно не для цільових, а для масових атак. Її мета полягає у зменшенні ризиків втрат від реалізованих атак. Дана КСЗІ реалізована як від внутрішніх загроз, таких як:

- системні адміністратори;
- власники файлів;
- власники програм;
- адміністратори застосунків;
- користувачі,

так і від зовнішніх - хакерів.

КСЗІ “Панцир+” може бути використана разом із ОС сімейства Windows, починаючи від Windows XP і закінчуючи Windows Server 2016. Дана СЗІ може бути використана для захисту хостів, таких як:

- ПЕОМ;
- робочі станції;
- сервери;
- термінальні сервери,

а також для засобів віртуалізації, включаючи захист як гостьових машин, так і гіпервізора.

Задачі захисту, які вирішує дана КСЗІ:

- захист від впровадження та виконання шкідливих програм та коду - вирішується задача захисту від несанкціонованого вторгнення та/або виконання командних файлів з правами користувача, адміністратора та системи; захисту від зараження легальних виконуваних і командних файлів;

- захист даних від атак на вразливості прикладного ПЗ - вирішується задача захисту даних, що опрацьовуються та системних об’єктів від загроз атак, що використовують вразливості прикладного ПЗ, включаючи фішингові атаки та атаки шифруючих вірусів;

- захист від атак на підвищення привілеїв - вирішується задача захисту від можливого отримання користувачем прав адміністратора, якому забороняється доступ до даних, які були створені інтерактивними користувачами, а адміністратором від отримання системних прав;

- захист даних від атак на вразливості системного ПЗ - вирішується задача захисту даних, що опрацьовуються, які були створені інтерактивними користувачами, від загроз атак, що використовують вразливості системного ПЗ (системних служб та процесів);

- захист від атак з боку санкціонованих користувачів - вирішується задача захисту від крадіжки даних інтерактивними користувачами, включаючи

привілейованих, розмежування прав та контроль роботи системних адміністраторів та адміністраторів застосунків.

Майже всі реалізовані у КСЗІ “Панцир+” технічні рішення є запатентованими. Також запатентованими є рішення, які плануються у подальшому внесенню до системи.

Зовнішній вигляд КСЗІ “Панцир+” можна побачити на наступних зображеннях:

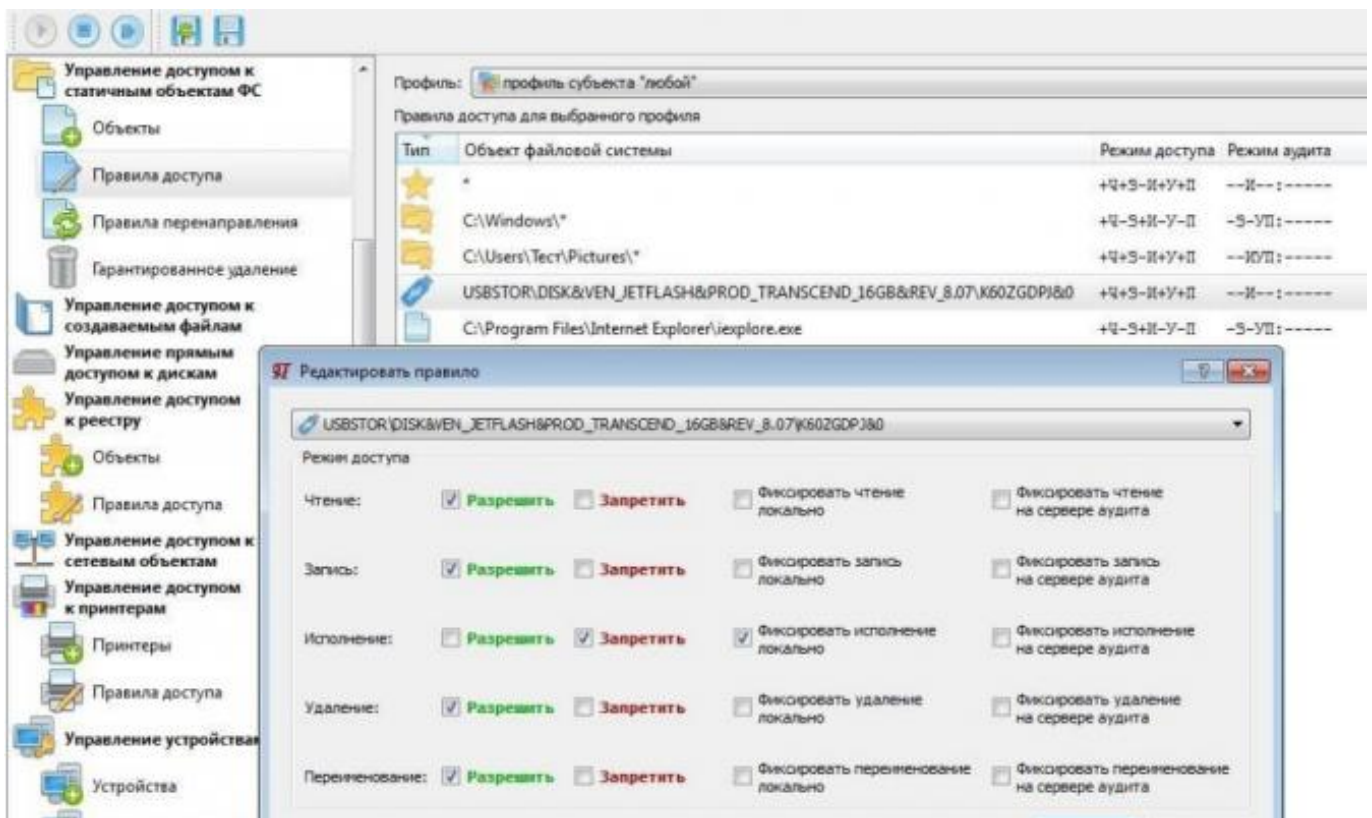


Рисунок 1.1 - Редагування правил доступу до носіїв інформації у КСЗІ “Панцир+”

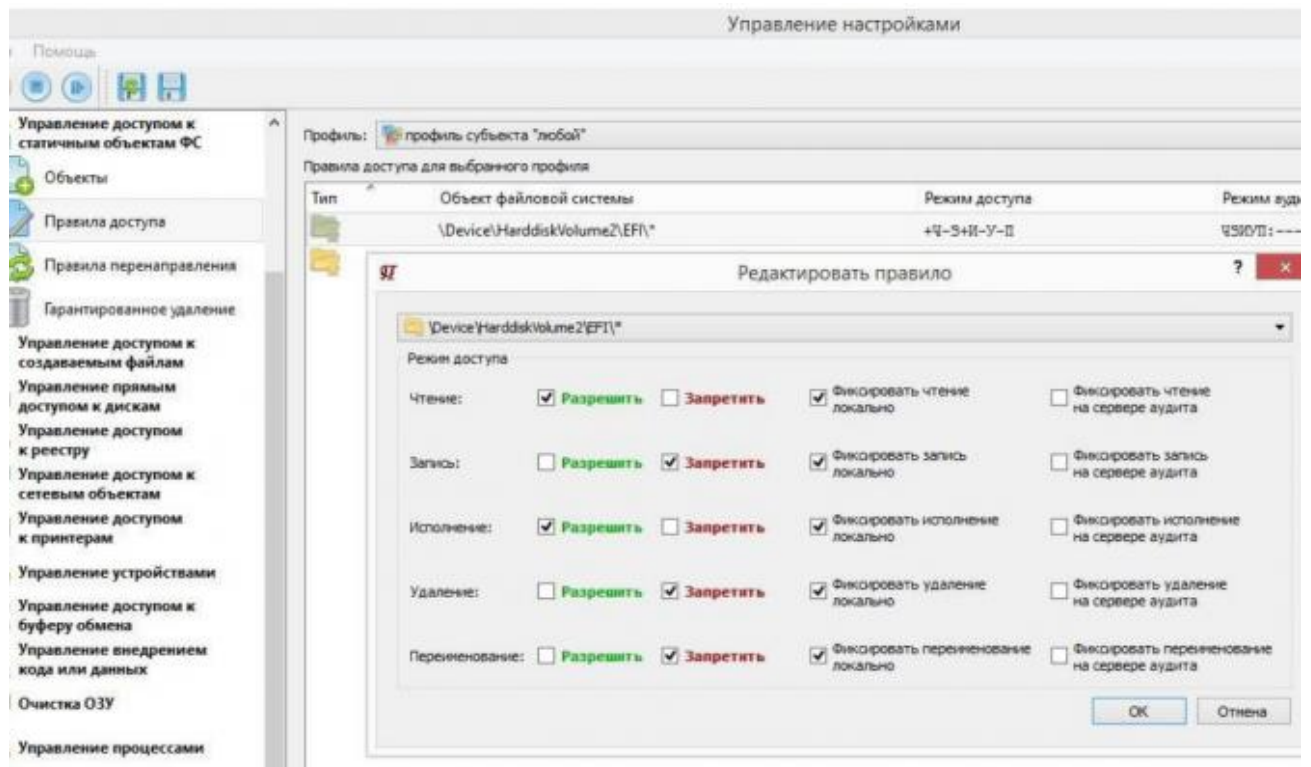


Рисунок 1.2 - Редагування правил доступу до об'єктів у КСЗІ "Панцирь+"

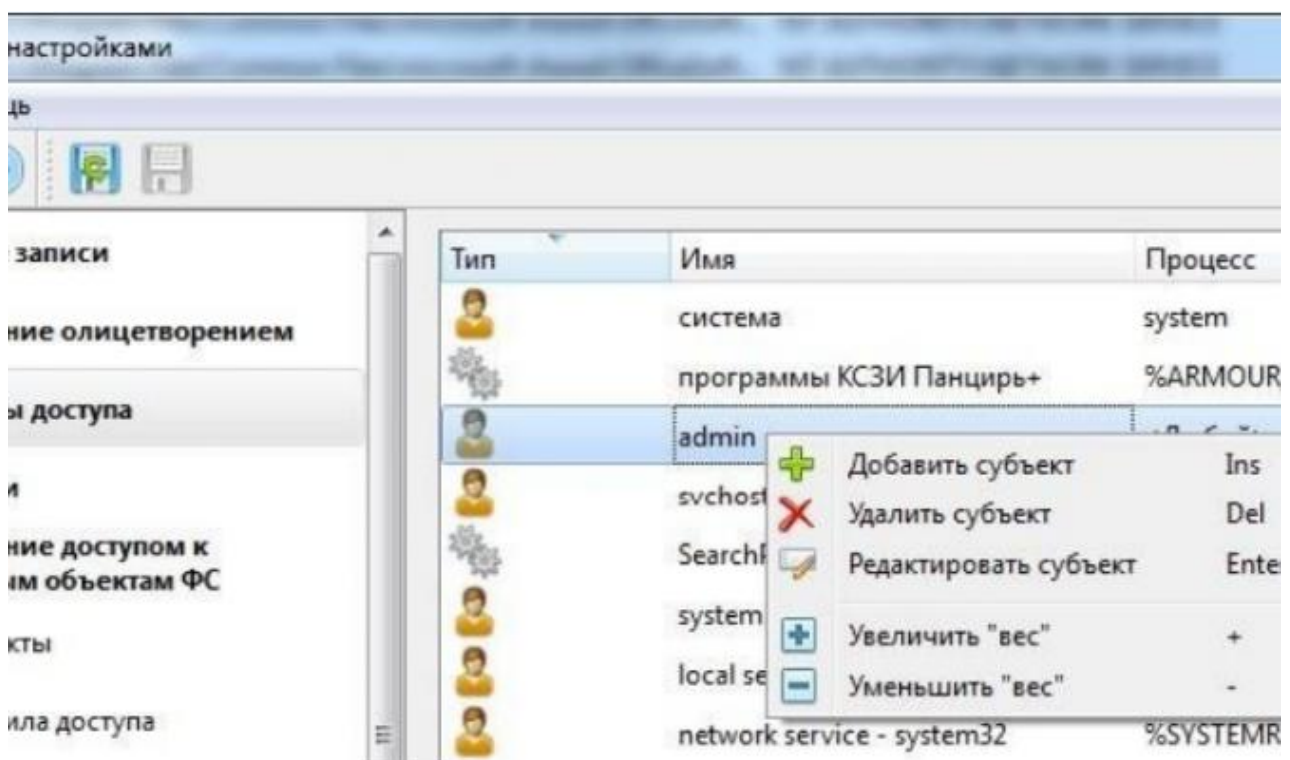


Рисунок 1.3 - Редагування ролей у КСЗІ "Панцирь+"

КСЗІ “Панцир+” - це мережева система захисту інформації, що реалізує клієнт-серверну архітектуру, до складу якої входять клієнтські частини (встановлюються на об'єктах захисту - вирішують задачі захисту інформації), сервери безпеки, що забезпечують віддалене адміністрування клієнтських частин КСЗІ “Панцир+” та інтерактивний режим опрацювання журналів аудиту подій безпеки, сервери аудиту (віддалений аудит подій безпеки у реальному часі).

КСЗІ “Панцир+” реалізує захист від хакерських атак у загальному вигляді - без використання засобів виявлення:

- забороняється будь-яка можливість, в тому числі з системними правами, виконання створених в процесі роботи виконуваних та командних файлів, будь-яка можливість, в тому числі, шляхом ін'єкції шкідливого коду у запущений процес, наділення програм шкідливими властивостями (це є основою антивірусного захисту у корпоративних застосунках);
- забороняється будь-яка можливість доступу потенційно вразливих застосунків (в тому числі браузерів у результаті фішингової атаки) до даних, які створюють інші застосунки у файлах та буфері обміну, будь-яка можливість доступу застосунків до попередньо створених даних, після прочитання застосунком даних, отриманих з критичних джерел (наприклад, у вигляді поштового вкладення у результаті фішингової атаки);
- розмежовуються права та контролюється доступ застосунків до критичних системних об'єктів - до альтернативних потоків, до метаданих, до іменованих каналів, до прихованих адміністративних загальних ресурсів, до завантажувальника ОС, до змінних BIOS UEFI, до об'єктів реєстру ОС тощо;
- забороняються можливі способи обходу розмежувальної та поділяючої політик доступу у результаті використання сервісів збільшення привілеїв, прямого доступу до дисків, доступу до залишкової інформації на диску, в результаті отримання системних прав тощо;
- забороняється доступ до даних, які були створені інтерактивними користувачами, з правами адміністратора та системними правами.

Оскільки більша частина цільових атак (більш ніж 80%) та витоку інформації (більш ніж 57%) здійснюються під привілейованим обліковим записом (як хакерська, так і інсайдерська атака), в КСЗІ “Панцир+” цьому питанню приділено особливу увагу.

За рахунок реалізації ефективного самозахисту, привілейований користувач (системний адміністратор, адміністратор застосунків тощо) може бути наділений тільки необхідними правами доступу, що не дозволяють отримати несанкціонований доступ до ІзОД та даних, що опрацьовуються. Реалізовані деякі засоби, що запобігають отриманню привілейованим користувачам системних прав. При цьому отримати НСД до ІзОД та даним, що опрацьовуються, не є можливим також і для системних процесів та служб.

Особливості КСЗІ “Панцир+” як сертифікованої СЗІ від НСД до ІзОД:

- реалізується не тільки розмежувальна (суб’єктів до об’єктів), а й розділююча (серед суб’єктів) політика доступу, що основана на автоматичній розмітці файлів, що створюються;
- суб’єкт доступу ідентифікується парою сутностей - користувач та процес, що у сучасних умовах є необхідним для реалізації ефективного захисту, оскільки загрозу може нести в собі як користувач, так і процес, при цьому суб’єкти та об’єкти доступу можуть задаватися у правилах доступу масками та змінними середовища;
- права доступу назначаються суб’єктам, а не в якості атрибутів об’єктам, що дозволяє реалізовувати рольову модель доступу - вирішується не задача захисту окремих об’єктів, як це робиться у інших СЗІ від НСД, а формування та розділення (для чого необхідна розділююча політика доступу) ролей працівників у інформаційній системі, з наданням їм тільки необхідних прав, що принципово відрізняє призначення КСЗІ “Панцир+” від інших СЗІ від НСД. Ця ж особливість реалізації дозволяє використовувати сервер системи захисту у якості повноцінного контролера домену безпеки у доменній мережі та забезпечує простоту тиражування налаштувань;

- реалізований механізм самозахисту не дозволяє впливати на КСЗІ “Панцир+” ні адміністраторам, ані системним процесам та службам, що забезпечує реалізацію наступних можливостей:

- реалізація рольової моделі доступу для системного адміністратора з можливістю обмеження його прав, включаючи доступ до даних, що опрацьовуються, та контролю його дій (можливість реалізації ієрархії адміністрування у інформаційній системі для привілейованих користувачів);

- обмеження можливостей системних процесів та служб, включаючи до себе заборону їм доступу до даних, що опрацьовуються.

1.1.2 КСЗІ “Secret Net Studio”

Одним за аналогів КСЗІ “Панцир+” є КСЗІ “Secret Net Studio”. [2] Secret Net Studio - це комплексне рішення для захисту робочих станцій та серверів на рівні даних, застосунків, мережі, операційної системи та периферійного обладнання. Продукт об’єднує в собі функціонал деяких засобів захисту “Коду Безпеки” (СЗІ від НСД Secret Net, мережевий екран TrustAccess, СЗІ Trusted Boot Loader), а також включає до себе низку нових засобів захисту.

В рамках даного продукту вирішуються наступні задачі:

- Захист від зовнішніх загроз:
 - Захист робочих станцій та серверів від вірусів та шкідливих програм
 - Захист від мережевих атак
 - Захист від підробки та перехоплення мережевого трафіку всередині локальної мережі
 - Захищений обмін даними з віддаленими робочими станціями
- Захист від внутрішніх загроз:
 - Захист інформації від НСД

■ Контроль витоків та каналів розповсюдження інформації, що захищається

■ Захист від дій інсайдерів

■ Захист від крадіжки інформації при втраті носіїв інформації

● Відповідність до вимог регуляторів - Secret Net Studio після отримання сертифікату дозволяє виконувати вимоги регуляторів під час атестації інформаційних систем, у яких опрацьовується конфіденційна інформація, на відповідність різноманітним вимогам держави.

Secret Net Studio 8.1 існує у двох варіантах виконання: автономний (передбачає тільки локальне управління захисними механізмами) та мережевий (передбачає централізоване управління захисними механізмами, а також централізоване отримання інформації та зміну стану ЕОМ).

В автономному варіанті захисні механізми встановлюються та управляються локально (без прив'язування до серверу безпеки). При такому використанні до складу продукту входять наступні компоненти:

● Клієнт - встановлюється на серверах та робочих станціях та передбачений для реалізації їх захисту;

● Центр управління (локальний режим) - програма управління в локальному режимі передбачає пряму роботу з елементами на ЕОМ;

● Сервер оновлення антивірусу - передбачений для забезпечення централізованої роздачі у локальній мережі оновлень баз даних ознак комп'ютерних вірусів для антивірусу за технологією ESET.

У мережевому варіанті захисні механізми встановлюються на всі сервери та робочі станції, при цьому здійснюється централізоване управління даними захисними механізмами. Як додаток до автономного варіанту, до мережевого варіанту входять:

● Сервер безпеки - є основним елементом, забезпечує взаємодію об'єктів управління, реалізує функції контролю та управління, а також опрацювання, зберігання та передачу інформації;

- Програма управління - встановлюється на робочих станціях адміністраторів та використовується для централізованого управління ЕОМ;
- Сервер аутентифікації - забезпечує роботу механізмів персонального мережевого екрану та авторизації мережевих з'єднань (входить до складу ПЗ серверу безпеки).

У Secret Net Studio забезпечується захист інформації на 5 рівнях, для кожного з яких існують певні захисні механізми (продукт об'єднує більш ніж 20 взаємно інтегрованих захисних механізмів). Інформація щодо рівнів захисту та відповідних їм механізмів знаходиться на рисунку 1.4.



Рисунок 1.4 - Рівні захисту та захисні механізми

Ліцензуються наступні компоненти системи:

- Захист від НСД до ІзОД (включає в себе механізми, що забезпечують захист входу до системи, довірену інформаційну середу, контроль витоків та каналів розповсюдження інформації, що захищається);

- Контроль пристроїв (входить до захисту від НСД, але може також бути придбаним окремо);
- Захист диску та шифрування контейнерів;
- Власний мережевий екран;
- Засіб виявлення та запобігання вторгнень;
- Антивірус;
- Шифрування мережевого трафіку.

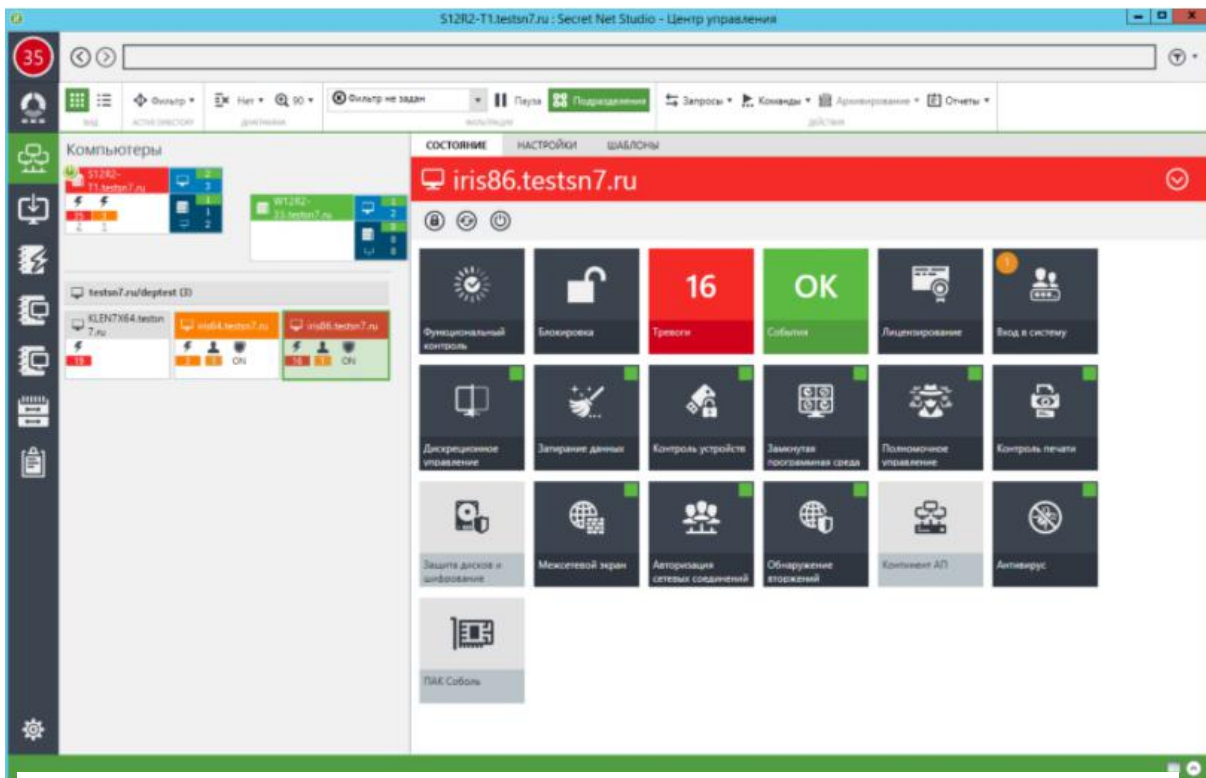


Рисунок 1.5 - Централізоване управління захисними компонентами Secret Net Studio

Захист входу до системи забезпечує запобігання доступу сторонніх осіб до ЕОМ. До механізму захисту входу відносять наступні засоби:

- Засоби для ідентифікації та автентифікації користувачів;
- Засоби блокування ЕОМ;
- Апаратні засоби захисту від навантаження ОС зі зйомних носіїв.

Ідентифікація та автентифікація виконуються при кожному вході до системи. У системі Secret Net Studio ідентифікація користувачів відбувається за одним з 3 (трьох) варіантів: за іменем (логін та пароль), за іменем або токеном, тільки за токеном.

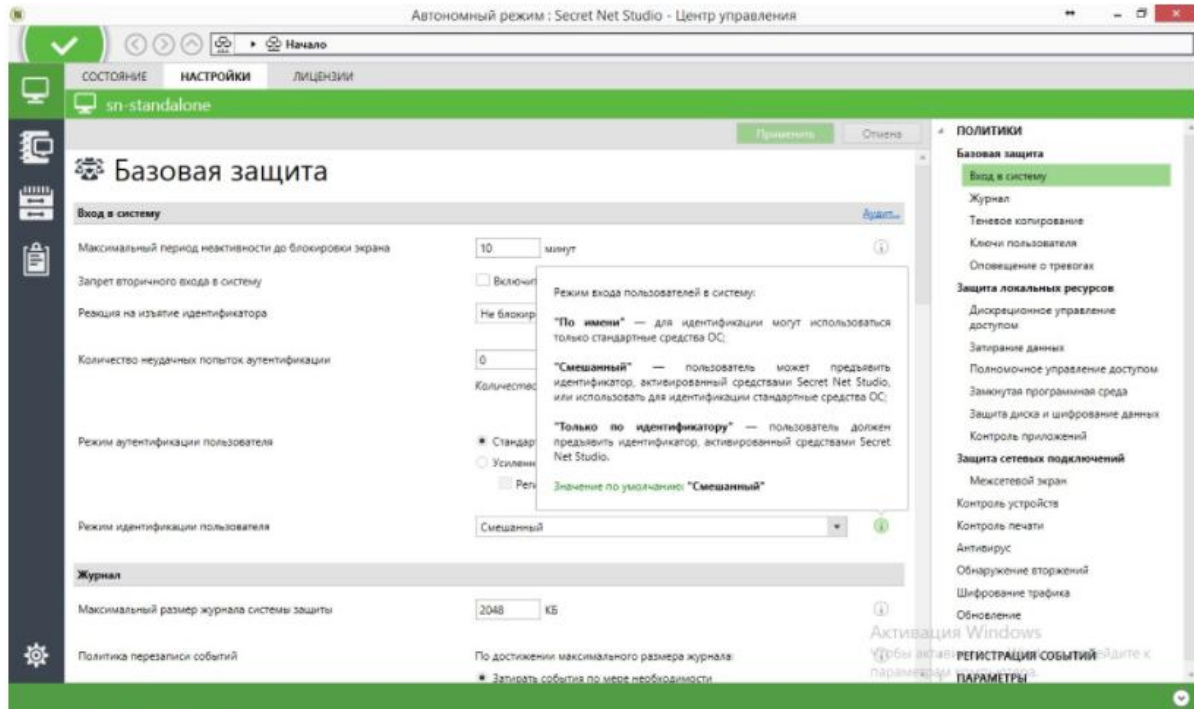


Рисунок 1.6 - Політики у Secret Net Studio

У Secret Net Studio 8.1 підтримується робота з наступними апаратними засобами:

- Засоби ідентифікації та автентифікації на базі ідентифікаторів eToken, iKey, Rutoken, JaCarta та ESMART;
- Засіб Secret Net Card;
- ПАК “Соболь”.

Засоби блокування ЕОМ призначені для запобігання його несанкціонованого використання. В цьому режимі блокуються засоби вводу (клавіатура та комп’ютерна миша) та екран монітору. Передбачені наступні варіанти:

- Блокування при невдалих спробах входу до системи;
- Тимчасове блокування ЕОМ;
- Блокування ЕОМ при спрацюванні захисних підсистем (наприклад, при порушенні функціональної цілісності системи);

- Блокування ЕОМ адміністратором оперативного управління.

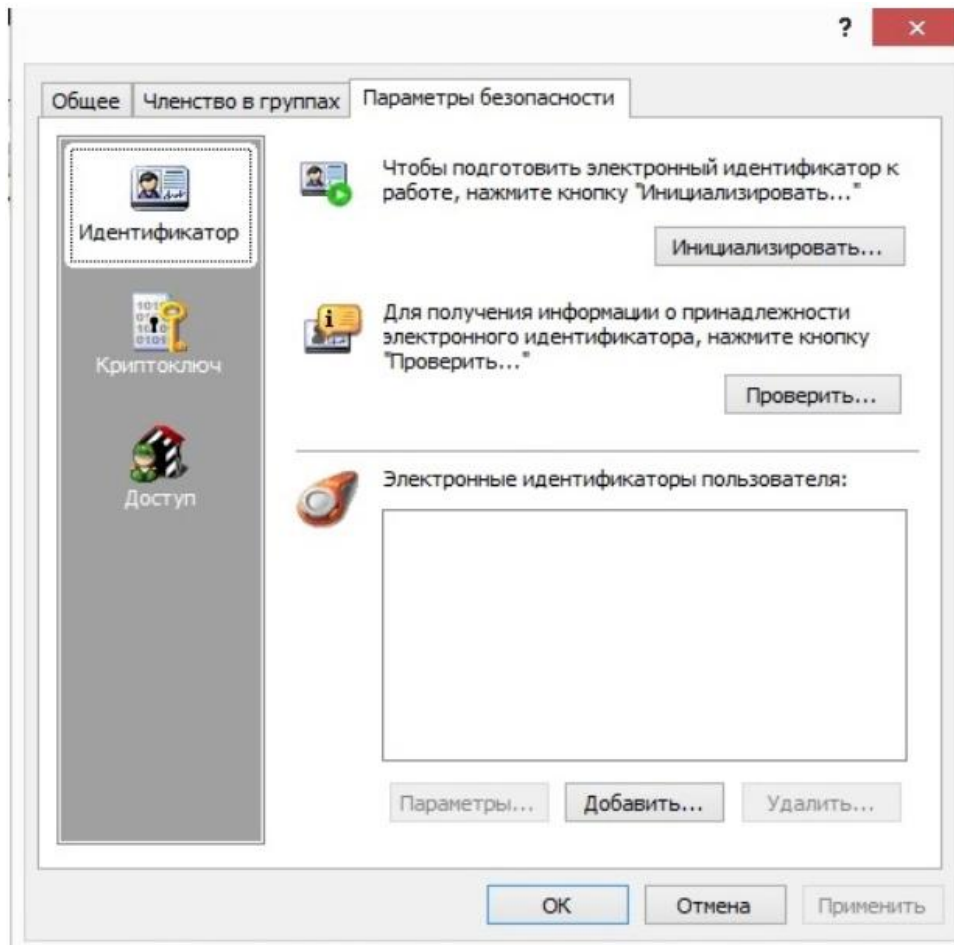


Рисунок 1.7 - Налаштування електронних ідентифікаторів для користувачів у Secret Net Studio

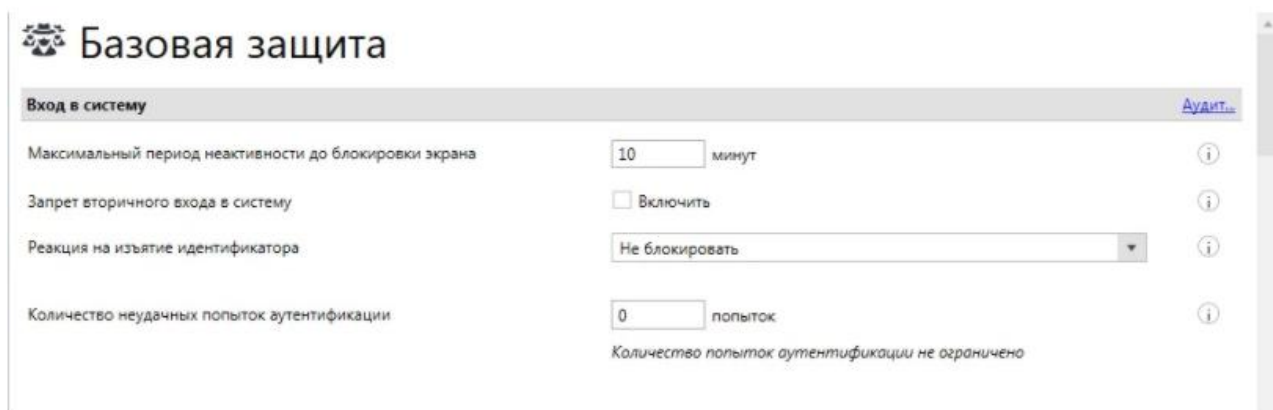


Рисунок 1.8 - Налаштування засобів блокування у Secret Net Studio

Функціональний контроль призначений для забезпечення гарантії того, що до моменту входу користувача до ОС усі ключові захисні підсистеми завантажені та функціонують. У випадку успішного завершення функціонального контролю цей факт реєструється у журналі Secret Net Studio. При невдалому завершенні реєструється подія з вказанням причин, вхід до системи дозволяється тільки користувачам за локальної групи адміністраторів ЕОМ.

Механізм контролю цілісності стежить за незмінністю об'єктів, що контролюються. Контроль проводиться у автоматичному режимі у відповідності до заданого розкладу. Об'єктами контролю можуть бути файли, каталоги, елементи системного реєстру та сектори дисків. При виявленні невідповідності можливі різноманітні варіанти реакції на ситуації порушення цілісності. Наприклад, реєстрація події у журналі Secret Net Studio та блокування ЕОМ. Вся інформація щодо об'єктів, методів, розкладу контролю зосереджена у моделі даних. Вона зберігається у локальній базі даних системи Secret Net Studio та являє собою ієрархічний перелік об'єктів з описом зв'язків між ними.

До складу системи Secret Net Studio 8.1 належить механізм дискреційного управління доступом до ресурсів файлової системи. Цей механізм забезпечує:

- розмежування доступу користувачів до каталогів та файлів на локальних дисках на основі матриці доступу суб'єктів (користувачів, груп) до об'єктів доступу;
- Контроль доступу до об'єктів при локальних чи мережевих зверненнях, включаючи звернення від імені системного облікового запису;
- Заборона доступу до об'єктів в обхід встановлених прав доступу;
- Незалежність дій від вбудованого механізму вибіркового розмежування доступу в ОС Windows. Це означає, що встановлені права доступу до файлових об'єктів в системі Secret Net Studio не впливають на аналогічні права доступу в ОС Windows та навпаки.

Крім того, користувачу надається можливість визначення облікових записів, котрим дані привілеї щодо управління правами доступу.

Механізм повноважного управління доступом забезпечує:

- Розмежування доступу користувачів до інформації, якій назначена категорія конфіденційності;
- Контроль підключення та використання пристроїв з назначеними категоріями конфіденційності;
- Контроль потоків конфіденційної інформації у системі;
- Контроль використання мережевих інтерфейсів, для яких вказані допустимі рівні конфіденційності сесій користувачів;
- Контроль друку конфіденційних документів.

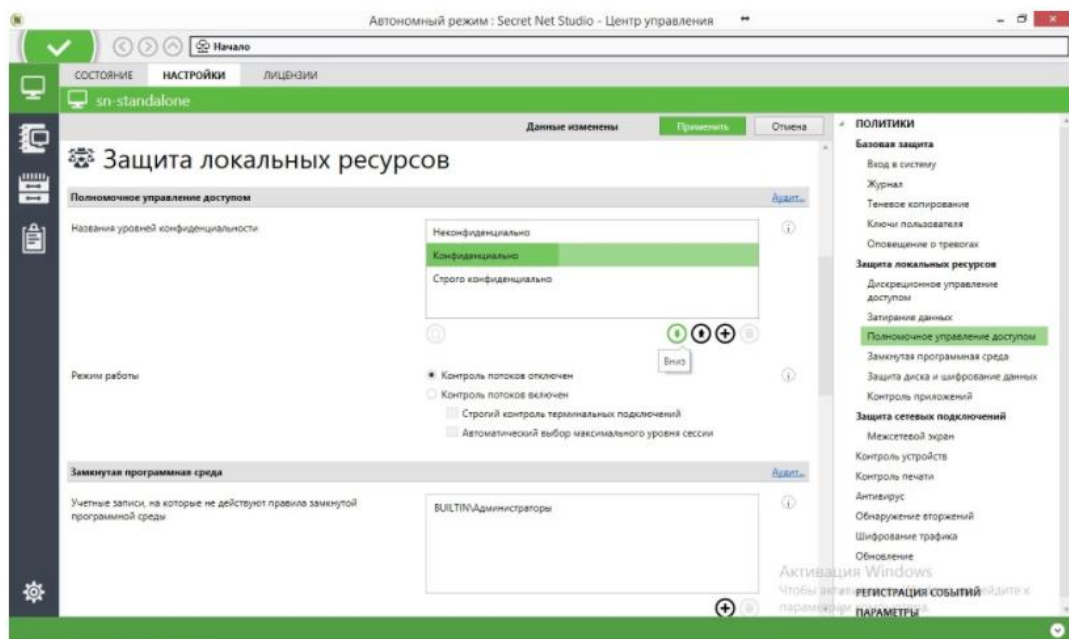


Рисунок 1.9 - Політики у Secret Net Studio

Для забезпечення функціонування механізму повноважного керування доступом при ввімкненому режимі контролю потоків, потребується виконати додаткове налаштування локально на ЕОМ. Для цього застосовується програма налаштування підсистеми повноважного керування доступом для режимів контролю. Налаштування відбувається перед увімкненням режиму контролю потоків, а також при додавання нових користувачів, програм, принтерів для оптимізації функціонування механізму. Доступ користувача до конфіденційної інформації здійснюється у відповідності до його рівня доступу. Наприклад, якщо рівень доступу користувача нижчий за категорію конфіденційності ресурсу - система блокує доступ до цього ресурсу.

Затирання інформації, що видаляється, робить неможливим відновлення та повторне використання даних після видалення. Абсолютне видалення досягається шляхом запису послідовності випадкових чисел на місце видаленої інформації у звільненій області пам'яті. Для більшої надійності може бути виконано декілька циклів затирання.



Рисунок 1.10 - Механізм затирання у Secret Net Studio

Механізм замкненої програмної середи дозволяє визначити для будь-якого користувача індивідуальний перелік дозволеного програмного забезпечення. Система захисту контролює та забезпечує заборону використання наступних ресурсів:

- Файлів запуску програм та бібліотек, що не входять до переліку дозволених для запуску та які не задовольняють певні умови;
- Сценарії, що не входять до переліку дозволених для запуску та не зареєстрованих в БД.

Спроби запуску недозволених ресурсів реєструються у журналі як події тривоги. На етапі налаштування механізму створюється перелік ресурсів, дозволених для запуску та виконання. Перелік може бути сформований автоматично на основі відомостей щодо встановлених на ЕОМ програм або за записами журналів, що містять відомості щодо запусків програм, бібліотек та сценаріїв. Також передбачена можливість формування переліку власноруч/

Захисний модуль “Антивірус” у Secret Net Studio 8.1 реалізує виявлення та блокування шкідливого коду за технологією ESET NOD32. Таким чином, Secret Net Studio дозволяє реалізовувати евристичний аналіз даних та автоматичну перевірку щодо наявності шкідливого ПЗ, зареєстрованого у базі сигнатур. При

спробі ЕОМ здійснюється сканування жорстких дисків, мережних папок, зовнішніх запам'ятовуючих пристроїв тощо. Це дозволяє виявити та заблокувати зовнішні та внутрішні мережні атаки, направлені на ЕОМ, що захищається. Завдяки використанню у рамках одного продукту СЗІ від НСД до ІзОД та антивірусу, час на перевірку та відкриття файлів складає на 30% менше, ніж при незалежній реалізації захисних механізмів. Оновлення антивірусу можна здійснювати як в режимі онлайн з серверів “Коду Безпеки” при підключенні ЕОМ до мережі Інтернет, так і з серверу оновлень компанії (у випадку, коли ЕОМ не має прямого доступу до мережі Інтернет). Адміністратору дозволене налаштування параметрів антивірусу за допомогою групових та локальних політик у програмі керування Secret Net Studio. Вся інформація щодо активностей механізму реєструється в журналі Secret Net Studio.

1.1.3 КСЗІ ВІ Dallas Lock

Для організацій, що планують використовувати віртуальні сервери для опрацювання конфіденційної інформації існує система захисту інформації у віртуальних інфраструктурах Dallas Lock[3] від компанії “Конфидент”. Розробник позиціонує своє рішення як систему для комплексного та багатофункціонального захисту конфіденційної інформації від несанкціонованого доступу у віртуальних середовищах на базі VMware vSphere 5.5. СЗІ ВІ Dallas Lock пройшла сертифікаційні іспити на відповідність 5 класу захищеності від НСД та 4 рівню контролю відсутності НДМ. СЗІ ВІ Dallas Lock можна використовувати для створення захищених автоматизованих систем до класу захищеності 1Г включно, для забезпечення 1 рівня захищеності особистих даних, в державних інформаційних системах 1 класу захищеності та автоматизованих систем керування технологічними процесами до 1 класу захищеності включно. СЗІ ВІ Dallas Lock реалізує наступні захисні міри: ідентифікація та автентифікація суб'єктів та об'єктів доступу, керування доступом до об'єктів віртуальної інфраструктури, реєстрація подій безпеки, забезпечення довіреного завантаження

серверів віртуалізації, контроль цілісності інфраструктури віртуалізації, резервування даних а також сегментування віртуальної інфраструктури.

В архітектурі C3I BI Dallas Lock присутні три модулі, та, в залежності від компоненту, змінюються вимоги щодо програмно-технічного забезпечення. Обов'язковою вимогою під час розгортання інфраструктури даної C3I BI є встановлення клієнтської частини C3I BI Dallas Lock 8.0 на сервер віртуалізації та сервер із встановленим компонентом СБ BI Dallas Lock для запобігання віддаленого НСД до VMware vCenter.

Технічний засіб із встановленим VMware vCenter Server 5.5 повинен мати наступний склад та характеристики програмно-технічного забезпечення:

- ОС: Microsoft Windows Server 2008 R2 64-bit (Standart, Enterprise, Datacenter, Web Server 2008, Storage Server 2008) або Microsoft Server 2021 64-bit (Foundation, Essentials, Standart, Datacenter);
- Процесор: Intel або AMD з двома логічними ядрами по 2 ГГц кожне;
- Оперативна пам'ять: мінімум 12 Гб;
- Вільне місце на диску: мінімум 60 Гб;
- Мережева карта.

Клієнтський модуль підтримує великий перелік популярних ОС:

- Windows XP (SP3) (Professional, Home, Starter);
- Windows Server 2003 (SP2) (Web, Standard, Enterprise, Datacenter);
- Windows Server 2003 R2 (SP2) (Web, Standard, Enterprise, Datacenter);
- Windows Vista (SP2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
- Windows Server 2008 (SP2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
- Windows 7 (SP1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (SP1) (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);

- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home).

СБ ВІ здійснює керування сервером vCenter та довіреними клієнтами керування vCenter. Мінімальна та оптимальна конфігурація ЕОМ для СБ ВІ визначається вимогами до версії ОС Windows, на котру встановлена клієнтська частина C3I Dallas Lock 8.0, на сервері необхідна наявність мережевої карти та USB-порту для використання апаратного ідентифікатора, що містить ліцензійний ключ.

Агент C3I ВІ встановлюється на гіпервізор VMware ESXi та є необхідним компонентом для захисту інформації у віртуальній інфраструктурі. Агент C3I ВІ Dallas Lock розгортається на гіпервізорі VMware ESXi для виконання частини функцій C3I на відповідному гіпервізорі.

Технічний засіб із встановленим гіпервізором VMware ESXi 5.5 повинен мати наступний склад та характеристики програмно-технічного забезпечення:

- Процесор: Intel або ADM з двома логічними ядрами по 2ГГц кожне, тільки x64;
- Оперативна пам'ять: мінімум 8 Гб;
- Вільне місце на диску: мінімум 60 Гб;
- Мережева карта.

В інфраструктурі C3I ВІ Dallas Lock , на автоматизованих робочих місцях, можливе застосування шаблонів налаштувань під різноманітні класи захищеності автоматизованих (інформаційних) систем згідно нормативно-правових актів. Адміністратор також може самостійно налаштувати систему під необхідний клас захищеності, використовуючи наступні сертифіковані механізми:

Управління пароллями. Оскільки використання продукту передбачає можливість подальшої атестації об'єкту інформатизації за вимогами безпеки, адміністратор домену безпеки може налаштувати параметри ідентифікації та

автентифікації користувачів: мінімальна довжина паролю, необхідність наявності у паролі чисел, спеціальних символів, ступінь відмінності нового паролю від старого та термін його дії. Окрім стандартного входу за паролем користувачам може бути назначений апаратний ідентифікатор.

Контроль цілісності. В C3I BI Dallas Lock реалізована система контролю цілісності системних файлів та конфігураційних файлів віртуальних машин на основі розрахунку контрольної суми за одним з обраних алгоритмів: CRC32, MD5, ГОСТ Р 3411-2012.

Розмежування доступу. В даній C3I можливо налаштувати правила розмежування доступу до компонентів віртуальної інфраструктури - до серверу віртуалізації та СБ BI, а також правила розмежування доступу за дискреційним принципом до об'єктів файлової системи та пристроїв у віртуальному середовищі (віртуалізоване обладнання) - на СБ BI та на сервері віртуалізації. Розмежування доступу до гіпервізорів ESXi та до віртуальних машин (файлам віртуальних машин) реалізується у межах рольової моделі розмежування доступу vSphere 5.5. Також можливий контроль доступу до операцій створення, запуску, зупинення та видалення віртуальних машин.

Мережевий екран. Через інтерфейс C3I BI можливо проводити налаштування правил фільтрації мережевого трафіку гіпервізору VMware ESXi.

Довірене завантаження. У випадку, коли цілісність конфігураційних файлів віртуальної машини порушена, функціональність довіреного завантаження віртуальної машини запобігає запуску гостьової ОС.

Реєстрація подій. Дана C3I дозволяє реєструвати та передивлятись події аудиту у 3 (трьох) журналах: журнал серверу безпеки віртуальної інфраструктури, журнал серверу віртуалізації та журнал гіпервізора. Для полегшення роботи із журналами є можливість фільтрації записів за певною ознакою, експортування журналів у різноманітні формати та виконання архівації журналів.

Збереження параметрів конфігурації. Існує можливість створення файлу конфігурації, який буде містити обрані адміністратором параметри.

Віддалене адміністрування. Можливе віддалене (мережеве) адміністрування СБ ВІ за допомогою консолі серверу безпеки.

1.2 Недоліки СЗІ на даному комунальному підприємстві

Особливість даного комунального підприємства полягає у тому, що воно є критично важливим для підтримання темпу життя у місті. Без цього підприємства важко уявити життя в будь-якому населеному пункті, численність населення якого вимірюється мільйонами людей, що вже казати про мегаполіс, який є столицею України. Дане комунальне підприємство містить велику кількість різноманітних служб, але нас цікавить лише одна - служба інформаційних технологій та зв'язку.

Основні функції даної служби полягають у забезпеченні надійної роботи, утриманні в технічно справному стані та розвитку пристроїв зв'язку, радіозв'язку, промислового телебачення, часофікації, автоматизованих систем управління технологічними процесами, автоматизованої системи оплати проїзду в метрополітені, пристроїв пасажирської автоматики та апаратно-програмних комплексів автоматизації виробничих процесів, мережевої інфраструктури, комп'ютерної, серверної та офісної техніки та програмного забезпечення інформаційних систем підприємства.

Через критичну важливість даного підприємства для комфортного життя людей, воно повинно бути захищене найсучаснішим програмним та технічним забезпеченням. Також повинна існувати СЗІ, яка запобігає великій кількості існуючих методів отримання НСД до ІзОД, що включає до себе засоби фізичного та програмного доступу. КП "Київський метрополітен" включає до себе велику кількість тісно пов'язаних між собою служб та відділів, які повинні бути належним чином захищені. У разі послабленого захисту одного з відділів потенційно можуть постраждати й інші відділи, що порушить роботу усього підприємства. Найгіршим існуючим варіантом наслідків порушення роботи

підприємства є втрата життя пасажирів, отже, до захисту інформації потрібно докласти максимум зусиль.

Я проходив практику у інженерно-технічному відділі, тож у дипломній роботі мною була розглянена СЗІ даного об'єкту. Протягом проходження переддипломної практики моя увага була зосереджена на технічному та програмному забезпеченні відділу даного підприємства. У таблиці 1.1 наведений перелік технічного забезпечення робочих місць.

Таблиця 1.1 - Технічне забезпечення робочих місць

№	Назва	Модель	Номер	Виробник
1	Системний блок	Optiplex 330	6Y8NB3J	Dell
	● Монітор	E1715Sc	F8S7M92	Dell
	● Клавіатура	KB-110X	XP163393106	Genius
	● Комп'ютерна миша	NetScroll 120	7 XP14CS9291 50	Genius
2	Системний блок	Optiplex 330	7B6HAG2Y	Dell
	● Монітор	SyncMaster 710v	GS17HSGY20625	Samsung
	● Клавіатура	RB216t	ONNV3G	Dell
	● Комп'ютерна миша	MSU1175	3H575B3209B	Lenovo
3	Сервер	PowerEdge T30	C9YFYH2	Dell
4	Мережевий екран	ASA5515-X	HGT65743IUY	Cisco

Однією з проблем СЗІ виявилась недостатня захищеність серверів, як серверів резервного копіювання, так і серверів, що опрацьовують та зберігають робочу інформацію. Проблема захищеності полягає у недоцільному розмежуванні прав доступу до технічного обладнання. Кожній системний адміністратор має достатній рівень повноважень для доступу до серверів. Якщо зловмисник отримає доступ до ЕОМ будь-якого адміністратора то він зможе й отримати доступ до серверів з інформацією з обмеженим доступом.

Другою проблемою програмного забезпечення виявився firewall, налаштований на мережевому екрані. Виявилось, що мережевий екран має невикористані відкриті порти. Нові засоби проникнення у систему виникають кожного дня, а відкриті порти збільшують ймовірність отримання зловмисником доступу до системи, і, як наслідок, корпоративної інформації.

На території об'єкту функціонує бездротова мережа Wi-Fi, тож слід розглянути загрози, пов'язані з цією мережею. У середовищі, у якому передаються сигнали через бездротову мережу, отримати доступ до інформації набагато простіше, ніж у провідних мережах, достатньо помістити антену в зону дії бездротової мережі. Також можливе клонування точки доступу. Зловмиснику потрібно лише забезпечити сигнал достатньої потужності у обраній зоні та дізнатися SSID точки, яку він збирається клонувати.

Не слід забувати також і про DoS-атаки. Частіше за все вони проводяться на базі WPA. Зловмисник кожену секунду надсилає два пакети з випадковими ключами шифрування, у результаті чого точка доступу, що приймає ці пакети, вирішує, що виконана спроба отримання НСД та закриває усі з'єднання.

Додатковою загрозою стає дозволена на території об'єкту політика BYOD - Bring Your Own Device. На жаль, не всі люди достатньо обізнані щодо безпеки поведінки в мережі Інтернет та можуть, самі того не помічаючи, завантажити на свій пристрій шкідливе ПЗ. При встановленні з'єднання власного пристрою та корпоративної мережі це шкідливе ПЗ може потрапити до мережі та інсталюватися на комп'ютери працівників або на сервери з важливою інформацією.

Між офісними кімнатами на об'єкті встановлені пластикові міжкімнатні перегородки, які не можуть забезпечити достатній рівень захисту витоку аудіо інформації. При обговоренні важливої інформації у офісі, вона може біти підслухана навіть без використання спеціальних апаратно-технічних засобів збору аудіо інформації.

Висновки до розділу 1

В даному розділі були розглянуті деякі з існуючих комплексних систем захисту інформації. Були досліджені можливості наведених прикладів існуючих комплексних систем захисту інформації, розглянуті їх функції та вимоги. Детально були розглянуті компоненти, наявні у наведених КСЗІ. Не слід забувати, що є можливість покращувати КСЗІ, додаючи до неї різноманітні ПАК, інсталиючи різноманітні додаткові програми, такі як системи IDS та IPS, додавати технічне забезпечення, таке як сервери та мережеві екрани. Аналіз існуючих КСЗІ показав, що існує велика кількість потенційних загроз та ризиків, які не беруться до уваги під час побудови СЗІ на підприємстві або у корпоративній мережі.

Жодна з наведених КСЗІ не спроможна забезпечити достатній рівень захисту на розглянутому підприємстві за різних причин, наприклад, застарілого ПЗ. Ще однією проблемою потрібно винести те, що дане підприємство працює як за фізичною, так і з віртуальною ІТ-інфраструктурою. Жодна з наведених КСЗІ не пропонує захист обох інфраструктур, а отже, потрібно або використовувати декілька готових рішень, додаючи до них різноманітні ПАК та ПЗ, або створювати окрему КСЗІ з оглядом на існуючі рішення. Також наведені СЗІ пропонують лише програмний захист інформації, в той час, як повноцінна КСЗІ передбачає також фізичні та інфраструктурні засоби запобігання витоку інформації.

2 ЕТАПИ СТВОРЕННЯ КСЗІ НА ПІДПРИЄМСТВІ КП “КИЇВСЬКИЙ МЕТРОПОЛІТЕН”

2.1 Обстеження середовищ функціонування ІТС

При виконанні цих робіт ІТС розглядається як організаційно-технічна система, що поєднує в собі комп'ютерні системи, фізичне середовище, середовище користувача, оброблену інформацію та технологію її обробки (далі - операційне середовище ІТС). [4]

Метою дослідження є опис форми кожного середовища ІТС для підготовки основних даних для формування вимог КСЗІ, виявлення елементів, які можуть прямо чи опосередковано впливати на інформаційну безпеку, виявлення взаємодії елементів різних середовищ та документація результатів дослідження для використання на наступних етапах.

Слід пам'ятати, що операційні середовища - це множини, що перетинаються, і їх різні елементи можуть одночасно міститися в різних середовищах і мати різні якості. Наприклад, програмне забезпечення може розглядатися комп'ютерною системою як об'єкт-процес, тоді як в інформаційному середовищі воно може розглядатися як пасивний об'єкт КС .

Обстеження виконується після розробки концепції ІТС (основні принципи та методи побудови), визначення основних завдань та характеристик ІТС, функціонального комплексу ІТС та коли існують варіанти їх реалізації.

Під час перевірки комп'ютерної системи слід проаналізувати та описати ІТС:

- загальний структурний план та склад (перелік та склад обладнання, технічного та програмного забезпечення, їхні зв'язки, особливості конфігурації, архітектура та топологія, програмне та програмно-апаратне забезпечення, апаратно-технічна інформаційна безпека, взаємне розміщення інструментів тощо);

- Типи та характеристики каналів зв'язку;
- особливості окремих компонентів та їх взаємовплив;
- Можливі обмеження щодо використання засобів тощо.

Необхідно виявити компоненти комп'ютерної системи, які містять і не містять засобів та механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні атрибути та характеристики, включаючи ті, що встановлені за замовчуванням. Метою цього аналізу є надання уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, що вимагають додаткових вимог до захисту, та реалізація додаткових заходів безпеки.

Під час перевірки інформаційного середовища вся інформація, яка обробляється та зберігається в ІТС (дані та програмне забезпечення), повинна бути проаналізована. У процесі аналізу інформація повинна класифікуватися відповідно до методу доступу та правової системи, а тип подання в ІТС (з точки зору КС) повинен бути визначений та описаний. Для кожного типу інформації та типів об'єктів, які вона містить, відповідають атрибути інформаційної безпеки (конфіденційність, цілісність, доступність) або КС (спостережливість). Аналіз технологій обробки інформації повинен розкрити характеристики електронних документів, визначити та описати інформаційний потік та середовище його передачі, джерело та призначення інформаційного потоку, принципи та методи управління інформаційним потоком, а також схему потоків. Записується тип носія інформації та порядок його використання під час роботи ІТС. Для кожного структурного елемента схеми інформаційного потоку склад інформаційного об'єкта, режим доступу до них, можливий вплив елемента середовища користувача на нього, фізичного середовища з точки зору збереження властивостей інформації.

Досліджуючи фізичне середовище, аналізується взаємне розташування засобів обробки інформації ІТС в інформаційній діяльності, зв'язку, системах життєзабезпечення та об'єктах зв'язку, а також режими роботи цих об'єктів. Процедура проведення обстеження повинна відповідати ДСТУ 3396.1 та розділу

про запобігання витоку інформації через технічні канали - НД ТЗІ 3.1-001.
Потрібно проаналізувати наступні характеристики фізичного середовища:

- географічне розташування компонентів ІТС (генеральне планування, планування сценаріїв); - територіальний захист та системи обходу;
- Категорійовані приміщення, де повинні знаходитись компоненти ІТС;
- режим доступу до компонентів фізичного середовища ІТС;
- фактори навколишнього середовища, щоб уникнути впливу технічної розвідки;
- існування засобів зв'язку, систем життєзабезпечення та елементів зв'язку поза зоною контролю;
- наявність та технічні характеристики системи заземлення;
- умови зберігання носіїв інформації, таких як магнітні, оптично-магнітні, паперові носії інформації тощо;
- наявність документації щодо проектування та експлуатації компонентів фізичного середовища.

Перевіряючи середовище користувача здійснюється аналіз:

- функцій та кількісного складу користувача, функціональні обов'язки та рівень кваліфікації;
- уповноваження користувачів отримати доступ до інформації, що обробляється в ІТС, отримати доступ до ІТС та її різних компонентів;
- Повноважень щодо управління КСЗІ;
- забезпечення можливостей різних типів користувачів, які надаються (можуть бути доступними) через засоби ІТС.
- існування СЗІ в ІТС.

Результати дослідження робочого середовища ІТС складаються у вигляді акту та, за необхідності, включаються до відповідної частини плану захисту інформації ІТС (далі - план захисту), який базується на НД ТЗІ 1.4 -001.

За результатами обстеження робочого середовища ІТС затверджується перелік об'єктів, що охороняються (враховуючи рекомендації НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також

визначаються потенційні інформаційні загрози, розробляється модель загроз та модель порушників. Модель виготовлена відповідно до норм НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Рекомендується представляти модель інформаційної загрози та модель порушника у вигляді окремих документів (або об'єднаних в один документ) плану захисту. [6]

На етапі формування завдання створення КСЗІ:

- визначено завдання захисту інформації Завдання в ІТС, мета створення КСЗІ, варіант вирішення проблеми захисту (згідно з ДСТУ 3396.1), основний напрямок захисту та обслуговування;
- проведений аналіз ризиків (вивчена модель загроз та модель порушника, можливі наслідки реалізації потенційних загроз, розмір можливих збитків тощо) для визначення переліку основних загроз;
- визначені загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації та допустимі обмеження використання певних заходів та засобів захисту (наприклад, обмеження використання активного захисту через ПЕМВН), інші обмеження середовища ІТС, обмеження використання ресурсів ІТС для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, впровадження та експлуатацію КСЗІ (різні підсистеми, компоненти), загальні вимоги щодо співвідношення та обмежень застосування організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації в її окремих підсистемах та компонентах, що стануть частиною КСЗІ.

Створюється звіт про виконання поточного етапу роботи та розробку додатків КСЗІ (створення тактико-технічних завдань КСЗІ або інших подібних документів, що замінюють його). [5]

2.2 Розробка політики безпеки інформації в ІТС

На етапі вивчення об'єкта, на якому створюється КСЗІ, розробники КСЗІ проводять детальне дослідження об'єкта, з'ясовують модель загрози, потенційні порушення та результати аналізу можливості керування ризиками, а також проводять додаткові дослідницькі роботи, пов'язані із пошуком шляхів реалізації завдання на створення КСЗІ, розробляють проект та звітність з НДР.

2.2.1 Оформлення політики безпеки

На цій стадії:

- Вибираються основні рішення для боротьби з усіма основними загрозами, формуються загальні вимоги, правила, обмеження, рекомендації тощо, які регламентують використання захищених технологій обробки інформації в ІТС, особисті заходи та засоби захисту інформації, а також види діяльності всіх користувачів;
- документи політики інформаційної безпеки.

Політику безпеки можна розробити для ІТС в цілому, або, якщо функції окремих компонентів КСЗІ є спеціальними, політики безпеки можна сформулювати для окремих компонентів, окремих функціональних завдань, окремих технологій обробки інформації тощо. Політика безпеки сформульована відповідно до норм НД ТЗІ 1.1-002 та рекомендацій НД ТЗІ 1.4-001. Рекомендується розробити стратегію безпеки у вигляді окремого документу Плану захисту. [6]

Положення політики безпеки пов'язані з рішеннями наступного етапу роботи (проектні рішення, організація роботи, визначення відповідальності, процедури впровадження та експлуатації КСЗІ тощо), які включені в документ для прийняття цих рішень на відповідний етап.

Як виняток, виконання роботи може бути включене до вимог технічного завдання на створення КСЗІ, а сама робота повинна проводитися відповідно до етапів, визначених ТЗ.

2.3 Розробка технічного завдання на створення КСЗІ

Технічне завдання для створення КСЗІ в ІТС є основним організаційно-технічним документом, який визначає вимоги щодо захисту інформації, що обробляється в ІТС, процедури створення КСЗІ, процедури проведення всіх видів випробувань та введення КСЗІ в експлуатацію.

Технічне завдання, яке використовувалося для створення КСЗІ, було сформульовано на відповідному етапі створення ІТС, враховуючи комплексний метод побудови КСЗІ. Він поєднує в собі всі необхідні заходи та засоби для запобігання різним загрозам інформаційній безпеці на різних етапах життєвого циклу ІТС. Технічне завдання, що використовується для створення КСЗІ, може бути розроблено для вперше створених ІТС та під час модернізації існуючих ІТС. Для оформлення ТЗ на КСЗІ існують наступні варіанти:

- у вигляді окремої частини ТЗ на створення ІТС;
- у вигляді окремого (часткового) ТЗ;
- як доповнення до ТЗ на створення ІТС.

Вибір варіантів не має обмежень.

Перший варіант рекомендується при створенні ІТС вперше. У разі модернізації КСЗІ, модернізації існуючих ІТС та ІТС, які вже затвердили ТЗ для створення, рекомендується другий або третій варіант, який не включає окрему частину із захисту інформації.

Для інтегрованих ІТС, заснованих на модульності, рекомендується формалізувати вимоги КСЗІ для кожного компонента ІТС в окремому документі. Допускається готувати один документ для кількох подібних компонентів КСЗІ (за винятком ТЗ що використовується для створення ІТС, окремого ТЗ) із зазначенням відмінностей чи особливостей.

Однотипними компонентами можна вважати КСЗІ ІТС, які забезпечують роботу комутаційних вузлів однієї і тієї ж мережі обміну даними, КСЗІ локальних мереж з однаковими функціональними завданнями інтегрованої ІТС тощо, якщо умови їх роботи суттєво не відрізняються. При цьому ТЗ включає вимоги до окремих компонентів ІТС та ІТС в цілому, а також вимоги щодо забезпечення безпечної взаємодії цих компонентів.

Єдиним обмеженням для розробки окремого ТЗ для створення КСЗІ або доповнення до ТЗ на створення ІТС є дотримання єдиної системи концепцій, імен, ідентифікацій об'єктів тощо, які використовуються в ТЗ на створення ІТС.

Для будь-якого з вищезазначених варіантів розробки та проектування ТЗ на КСЗІ його зміст, порядок погодження та затвердження повинні відповідати НД ТЗІ 3.7-001 та ГОСТ 34.602.

2.4 Розробка проекту КСЗІ

Проект КСЗІ ґрунтується на ТЗ на створення ІТС (додаток до нього, окреме ТЗ, яке використовується для створення КСЗІ).

Під час розробки проекту КСЗІ були формулюються та підтверджуються проектні рішення для досягнення вимог ТЗ, забезпечення сумісності та взаємодії різних компонентів КСЗІ, а також різних заходів та методів захисту інформації.

Проекти КСЗІ реалізується на таких етапах створення ІТС: ескізний проект, технічний проект та робочий проект.

Дозволяється виключати етап "Ескізний проект КСЗІ" та об'єднати "Технічний проект КСЗІ" та "Робочий проект КСЗІ" в один етап "Техно-робочий проект КСЗІ".

Для всіх етапів розробки проекту КСЗІ склад документа визначається ТЗ, види та зміст - ГОСТ 34.201, НД ТЗІ 2.5-004. Документація до програмного забезпечення реалізована відповідно до набору стандартів ESDP, а документація до обладнання - відповідно до набору стандартів ESCD. [7]

На етапі створення ескізного проекту КСЗІ приймається попереднє проектне рішення КСЗІ та, за необхідності, формулювання його окремих компонентів, а також розробка, оформлення, узгодження та затвердження документа на КСЗІ. Зміст та стиль документа повинні бути достатніми для повного опису проектних рішень на рівні ескізного проекту.

Визначаються:

- загальна функція КСЗІ та функції різних її компонентів;
- склад комплексу захисту інформаційних технологій для запобігання витоку технічними каналами та спеціальним впливам;
- склад заходів протидії технічним, розвідкам, організаційним, правовим та інших захисних заходів;
- склад КЗЗ;
- узагальнена структура та схема взаємодії компонентів КСЗІ.

Надаються попередні технічні рішення, завдяки яким можуть бути реалізовані завдання та функції КСЗІ.

Розробка проектних рішень КСЗІ. Виконується розробка: загальних проектних рішень, необхідних для реалізації вимог ТЗ на КСЗІ; визначення структури КСЗІ (організаційна структура, апаратна та програмна структура), алгоритмів роботи та умов використання засобів захисту; архітектура КЗЗ, визначена функціональним профілем послуг безпеки інформації та механізми реалізації.. Згідно з НД ТЗІ 2.5-004, НД ТЗІ 2.5-007, НД ТЗІ 2.5 -008, НД ТЗІ 2,5-010 вживаються організаційні та технічні заходи для забезпечення послідовності розробки КЗЗ, архітектури, середовища розробки, тестування, експлуатаційного середовища та експлуатаційних документів КЗЗ.

Розробка документації в КСЗІ. Проводиться розробка, оформлення, узгодження та затвердження кількості документів, передбачених ТЗ на КСЗІ. Зміст і стиль документа повинні бути достатніми для повного опису проектних рішень на рівні технічного проектування.

Розробка документації на постачання засобів захисту інформації та / або технічних вимог (технічних завдань) на їх розробку. Для комплектації КСЗІ,

готуються та оформлюються документи на постачання захисного обладнання або продуктів, що включаються до її складу. Якщо необхідного товару немає на ринку захисних заходів, визначаються технічні вимоги (технічні завдання) на розробку відповідних заходів.

Розробіть завдання на проектування в суміжних частинах. Здійснюється розробка, проектування та затвердження проектних завдань, пов'язаних зі створенням КСЗІ, або суміжних питань, що впливають на умови її експлуатації (будівництво, електротехнічні, санітарно-технічні та інша підготовчі роботи).

На етапі створення робочого проекту КСЗІ розробляється, реєструється та затверджується робоча та експлуатаційна документація КСЗІ, та, за необхідності, окремі її компоненти. Робочі документи містять детальні рішення щодо реалізації технічних проектів КСЗІ, забезпечення управління КСЗІ та взаємодії її компонентів, а також документи, необхідні для тестування, налагодження та тестування КСЗІ.

Проводиться розробка засобів захисту інформації або адаптується готовий продукт до умов експлуатації КСЗІ. Розробка методів захисту інформації від НСД відбувається згідно з НД ТЗІ 3.6-001.

Робочі документи з технічного захисту для запобігання витоку інформації через технічні канали повинні включати схеми розміщення ОТЗ ІТС, кабельного обладнання, мережі електроживлення та системи заземлення. Ці плани реалізуються відповідно до вимог ТР ЕОТ-95, ТТР ТЗІ-ПЕМВН-95, СТР-2, СТР-3, НД ТЗІ 3.3-001, НД ТЗІ 2.4-007, СВТР-78. Враховуються умови їх розміщення та мінімально допустимі відстані між цими пристроями та ДТЗ (зв'язок, системи та засоби кондиціонування повітря, сигналізація, світло, радіо тощо), розташованих у приміщенні, де знаходиться обладнання ІТС, та в суміжних приміщеннях. Ці умови розміщення та мінімально допустимі відстані, взяті з експлуатаційних документів, що додаються до сертифікованого ОТЗ. Якщо ОТЗ, що використовується як частина КСЗІ, не має сертифікатів відповідності вимогам до технічного захисту інформації, мінімально допустимі відстані та інші умови

розміщення цих засобів повинні бути визначені за результатами їх спеціальних досліджень.

До складу робочої документації на KZZ необхідно включити опис процедури встановлення та ініціалізації комплексу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контролю за діями користувачів, формування та актуалізації БД захисту, а також контролю цілісності програмного забезпечення та БД захисту. Документація робочого проекту повинна містити вихідні дані для внесення їх до БД захисту.

Експлуатаційна документація включає опис функціонування КСЗІ та настанови (інструкції) щодо забезпечення цього порядку обслуговуючим персоналом та користувачами, порядку супроводження КСЗІ впродовж життєвого циклу ІТС.

2.5 Підготовка КСЗІ до введення в дію

Проводяться роботи з підготовки організаційної структури та готуються розпорядчі документи щодо управління інформаційною системою ІТС.

Якщо це не було зроблено на попередніх етапах, створюється СЗІ (призначається відповідальний за захист інформації співробітник).

Підготовка та затвердження документів, що містяться в Плані захисту, повинні бути завершені (за винятком тих, що потребують результатів наступних етапів робіт).

Створення СЗІ та формування Плану захисту здійснюється згідно з НД ТЗІ 1.4-001.

2.6 Навчання користувачів

Усі категорії користувачів ІТС (персонал технічної служби, звичайні користувачі та користувачі, уповноважені керувати об'єктами КСЗІ) проходять навчання щодо основних положень документа Плану захисту, які необхідні їм для

дотримання правил політики безпеки інформації, оботі інструменту захисту тощо для перевірки їхньої здатності використовувати впроваджену технологію захисту інформації та реєстрації результатів навчання.

2.7 Попередні випробування

Метою попереднього випробування є перевірка ефективності роботи КСЗІ та визначення можливості прийняття її в дослідну експлуатацію. Під час випробування перевіряється працездатність КСЗІ та чи відповідає вона вимогам ТЗ.

Попередні випробування виконуються відповідно до процедур та методів випробувань. Процедури та методи випробування готуються розробниками КСЗІ та узгоджуються замовниками ІТС. Процедури та методи випробувань, а також протоколи випробувань сформульовані та видані відповідно до вимог РД 50-34.698.

Попереднє випробування організовується замовником ІТС і проводиться розробником КСЗІ разом із замовником. Замовники ІТС створюють комісію для проведення попередніх випробувань. Представником замовника призначається голова комісії.

Результати попереднього випробування записуються в "Протокол випробування", який містить висновки щодо можливості прийняття КСЗІ у дослідну експлуатацію, а також перелік виявлених недоліків, необхідні заходи щодо їх усунення та рекомендовані терміни виконання робіт.

Після усунення існуючих недоліків та коригування проектних, робочих та експлуатаційних документів КСЗІ формулюється акт прийому КСЗІ у дослідну експлуатацію.

2.8 Дослідна експлуатація

Під час дослідної експлуатації КСЗІ відпрацьовуються такі технології, як обробка інформації, обіг машинних носіїв даних, керування засобами захисту, розмежування прав доступу користувачів до ресурсів ІТС та автоматизований контроль поведінки користувачів; співробітники ІТС та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційно-розпорядчих документів щодо розподілу технічних засобів та прав доступу до інформаційних ресурсів; здійснюється (за потреби) вдосконалення програмного забезпечення, додаткове налагодження та конфігурація КЗЗ; виконується (за необхідності) коригування робочих та експлуатаційних документів.

На основі результатів роботи за довільною формою формулюється акт про завершення дослідної експлуатації, яка містить висновок про можливість (неможливість) подання КСЗІ на державну експертизу. [8]

2.9 Державна експертиза КСЗІ

Державна експертиза КСЗІ є окремим етапом іспиту ІТС.

Метою перевірки є встановлення, чи відповідає КСЗІ технічним завданням та вимогам НД щодо захисту інформації, та визначається можливість введення КСЗІ в складі ІТС в експлуатацію. Державна експертиза КСЗІ в ІТС проводиться відповідно до Положення про державну експертизу у сфері технічного захисту інформації.

Дефекти, виявлені під час перевірки стану, усуваються до завершення, а процедура усунення така ж, як і для попередніх тестів. Якщо з якихось причин недоліки в процесі перегляду не можуть бути усунені, оформлюється акт, який включає перелік необхідних удосконалень та рекомендації щодо їх виконання. Після завершення роботи, передбаченої актом, проводиться повторна експертиза.

Для інтегрованих ІТС перевірка кожного компонента (модуля) КСЗІ може здійснюватися окремо. Перевірка КСЗІ інтегрованої ІТС полягає у перевірці взаємодії вже оцінених модулів (адміністрування, обмін даними БД безпеки тощо). Документи, що містять результати робіт різних етапів для КСЗІ ІТС (протоколи, акти, сертифікати відповідності), оформлюються з урахуванням відповідних документів на компоненти КСЗІ.

Якщо інтегрована КСЗІ містить стандартні модулі, створені для одного ТЗ, експертиза таких модулів КСЗІ проводиться у два етапи: перший етап - це всебічна перевірка обраного стандартного модуля, а другий етап - перевірка на відповідність умови експлуатації для кожного конкретного об'єкта всіх модулів КСЗІ цього типу.

Впровадження нових (оцінених) модулів в існуючу КСЗІ не вимагає повторної перевірки всієї КСЗІ. Оцінюється взаємодія нового модуля з компонентом КСЗІ, що вже знаходиться в експлуатації.

Дозволяється починати виконувати перевірку стану КСЗІ паралельно з роботою етапів проектування.

У першу чергу рекомендується застосовувати цю процедуру для складних з точки зору архітектури, складу та обсягу робіт КСЗІ. При цьому експерти послідовно оцінюють технічні та організаційні рішення на всіх етапах роботи. Це дозволяє швидко усунути недоліки та скоротити час проведення експертизи, яку можна завершити до етапу приймальних випробувань ІТС.

Приймальні випробування ІТС проводяться при функціонуючій КСЗІ.

Робота виконується з використанням тестових даних, які не містять ІзОД.

2.10 Супроводження КСЗІ

Відповідно до Плану захисту та експлуатаційних документів на компоненти КСЗІ виконуються роботи з організаційного забезпечення функціонування КСЗІ, управління засобами захисту інформації, післягарантійного обслуговування.

Висновки до розділу 2

У цьому розділі були детально досліджені усі етапи побудови КСЗІ на підприємстві. Були розглянуті документи, які створюються у процесі побудови КСЗІ, проаналізовані характеристики фізичного середовища, документи, згідно яким розробляється політика безпеки, винятки під час розробки КСЗІ. Детальний аналіз показав, наскільки багато потрібно зробити для того щоб побудувати КСЗІ та отримати атестат. Під час дослідження були розглянуті різноманітні нормативно правові акти та норми НД ТЗІ, наведені питання, за якими визначається необхідність створенні КСЗІ на об'єкті захисту.

3 РОЗРОБКА УДОСКОНАЛЕНОЇ КСЗІ ДЛЯ КОМУНАЛЬНОГО ПІДПРИЄМСТВА “КИЇВСЬКИЙ МЕТРОПОЛІТЕН”

3.1 Аудит інформаційної безпеки комунального підприємства

Аналіз інформації, яка циркулює у комунальному підприємстві, дозволяє визначити, яку інформацію слід захищати та яким чином побудувати захист. Основною задачею даного аналізу є виявлення повного переліку джерел та носіїв інформації та визначення структури конфіденційності інформації.[9]

У даному комунальному підприємстві присутні дані, що складають державну таємницю. До відомостей, які потрібно захищати, відносяться конфіденційні документи. Під конфіденційним документом мається на увазі оформлений необхідним чином носій документованої інформації, що містить відомості обмеженого доступу чи використання, який складає інтелектуальну власність юридичної чи фізичної особи.

Таблиця 3.1 - Елементи захисту.

№	Назва елементу інформації	Конфіденційність інформації	Назва джерела інформації	Місцезнаходження інформації
1	Дані щодо клієнтів	Конфіденційно	Працівники, документи, відходи	Бухгалтерія
2	Службові записи	Конфіденційно	Працівники, документи, відходи	Кабінет директора
3	Накази	Конфіденційно	Працівники, документи, відходи	Кабінет директора

Кінець таблиці 3.1

4	Звіти	Конфіденційно	Працівники, документи, відходи	Кабінет директора
5	Документи щодо мобілізаційної роботи	Державна таємниця	Працівники, документи, відходи	Режимно-секретний відділ
6	Накази щодо цивільної оборони	Державна таємниця	Працівники, документи, відходи	Режимно-секретний відділ
7	Фінансові звіти	Конфіденційно	Працівники, документи, відходи	Бухгалтерія
8	Податкові декларації	Конфіденційно	Працівники, документи, відходи	Бухгалтерія

Задля визначення вимог до ІС скористуємось двома документами: “Автоматизовані системи. Захист від НСД до ІзОД. Класифікація автоматизованих систем та вимоги щодо захисту інформації”, “Засоби обчислювальної техніки. Мережеві екрани. Захист від НСД до ІзОД. Показники захищеності від НСД до ІзОД”.

Загроза безпеки інформації - можливість виникнення такої події, наслідком якої може бути небажаний вплив на інформацію: порушення фізичної цілісності, логічної структури, несанкціонована модифікація інформації, несанкціоноване отримання інформації, несанкціоноване поширення інформації.[8] Загрози безпеці, актуальні для даного комунального підприємства:

- Відмова у роботі апаратури;
- Помилки або навмисні дії працівників інформаційної системи;
- Помилки адміністрування;
- НСД до ІзОД у місцях необмеженого доступу;

- НСД до ІзОД через втрату або крадіжку носія;
- НСД до ЕОМ внаслідок цільової атаки на ІС;
- НСД до паперових інформаційних ресурсів у приміщенні підприємства;
- Порушення конфіденційності електронної документації;
- Пожежі;
- Втрата або крадіжка документів;
- Стихійні лиха;

У таблиці 3.2 наведений зразок загроз та вразливостей ІБ підприємства у відповідності до описаних загроз.

Таблиця 3.2 - Аналіз вразливостей комунального підприємства

№	Загрози	Вразливості
1	Відмови у роботі апаратури	Помилки у ОС або ПЗ
		Ненадійність окремих вузлів апаратури: мікропроцесорів, жорстких дисків, відеоадаптерів, мережевих карт, комутаторів
		Нестабільність електропостачання
		Неправильні дії з боку обслуговуючого персоналу
		Втрата електронних документів
2	Помилки або навмисні дії працівників ІС	Неправильні дії користувачів внаслідок недостатньої кваліфікації
		Навмисні дії персоналу
3	Помилки адміністрування	Неправильні дії адміністратора внаслідок недостатньої кваліфікації
4	НСД до ІзОД у місцях необмеженого доступу	Необмежений доступ до інформації сторонні осіб
5	НСД до ІзОД внаслідок помилок користувачів	Помилки користувачів

Кінець таблиці 3.2

6	НСД до ІзОД через втрату носія	Можливість втрати або крадіжки носія інформації
7	НСД до електронних інформаційних ресурсів внаслідок цільової атаки на ІС	Помилки адміністратора
		Наявність НДМ ПЗ
		Нестійкість алгоритмів перед впливом шкідливого ПЗ
8	НСД до паперових інформаційних ресурсів у приміщенні керування	Відсутність інженерно-технічного захисту
		Незахищеність носіїв
9	Порушення конфіденційності електронної документації	Відкритий трафік
		Атаки на ІС
10	Стихійні лиха	Відсутність плану евакуації
		Блокування шляхів евакуації
11	Пожежі	Відсутність пожежної системи
		Несправний стан електросистем будівель та споруд
12	Втрата, крадіжка паперових документів	Відсутність технічних систем охорони
		Низька відповідальність служби безпеки

Після оцінки загроз безпеки необхідно запропонувати методи нейтралізації цих загроз. Вразливості та методи їх запобігання наведені у таблиці 3.3

Таблиця 3.3 - Вразливості та методи їх запобігання

№	Вразливість	Метод запобігання
1	Помилки у ОС або ПЗ	● Інсталювання оновлень ОС, ПЗ, сервісних пакетів, виправлень тощо ● Використання перевіреного ПЗ
2	Ненадійність окремих вузлів апаратури	● Контроль роботи апаратури ● Заміна або ремонт апаратури, що вийшла з ладу
3	Нестабільність електропостачання	● Використання засобів стабільного електропостачання
4	Знищення електронної документації	● Використання засобів резервного копіювання
5	Помилки у роботі працівників внаслідок недостатньої кваліфікації	● Навчання персоналу ● Розмежування повноважень персоналу ● Прийом на роботу кваліфікованих спеціалістів ● Контроль роботи персоналу
6	Навмисні дії персоналу	● Розмежування повноважень персоналу ● Контроль роботи персоналу
7	Необмежений доступ до інформації сторонніх осіб	● Розміщення моніторів на робочих місцях, що не допускають зйому відеоінформації з нього
8	Можливість втрати або крадіжки носія інформації	● Облік носіїв інформації ● Видача носіїв під розпис
9	Необмежений доступ до засобів друку та копіювання	● Контроль доступу до засобів друку

При опрацюванні особистих даних у розподілених ІС особистих даних, що мають підключення до мереж зв'язку загального користування та (або) мереж

міжнародного інформаційного обміну можлива реалізація наступних загроз безпеки особистих даних:

- Загрози витоку інформації по технічним каналам;
- Загрози НСД до особистих даних, що опрацьовуються на автоматизованому робочому місці.

Загрози витоку інформації по технічним каналам містять:

- Загрози витоку акустичної (мовної) інформації;
- Загрози витоку візуальної інформації;
- Загрози витоку інформації по каналу побічних електромагнітних випромінювань.

● Виникнення загроз витоку акустичної інформації можливе за наявності засобів мовного вводу особистих даних до ІС або функцій відтворення особистих даних акустичними засобами ІС.

● Реалізація загрози витоку візуальної інформації можлива за рахунок перегляду інформації за допомогою оптичних (оптоелектронних) засобів з екранів моніторів та інших засобів відображення обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів опрацювання графічної, відео- та буквено-цифрової інформації, що входять до складу ІС.

● Загрози НСД пов'язані з діями порушників, що мають доступ до ІС, включаючи користувачів ІС, що реалізують загрози безпосередньо у ІС, а також порушників, що не мають доступу до ІС, що реалізують загрози із зовнішніх мереж зв'язку загального користування.

● В таких інформаційних системах можливі:

● Загрози, що реалізуються в ході завантаження ОС та направлені на перехоплення паролів та ідентифікаторів, модифікацію базової системи вводу\виводу (BIOS), перехоплення керування завантаженням;

● Загрози виявлення паролів;

● Загрози, що реалізуються після завантаження ОС та направлені на виконання НСД із застосуванням стандартних функцій (знищення, копіювання, переміщення, форматування носіїв інформації тощо) ОС або будь-якої

прикладної програми (системи керування БД), із застосуванням спеціально створених для отримання НСД програм;

- Загрози впровадження шкідливих програм;
- загрози “аналізу мережевого трафіку” з перехопленням інформації, що передається до зовнішніх мереж та отримується із зовнішніх мереж;
- Загрози сканування, направлені на виявлення типу ОС, мережеских адрес робочих станцій, топології мережі, відкритих з’єднань тощо;
- Загрози отримання НСД шляхом заміни довіреного об’єкту;
- Загрози типу “Відмова в обслуговуванні”;
- Загрози віддаленого запуску застосунків;
- Загрози нав’язування хибного маршруту шляхом несанкціонованої зміни маршрутно-адресних даних як всередині мережі, так і у зовнішніх мережах.

Актуальною вважається загроза, яка може бути реалізована та передбачає небезпеку. Для оцінки реалізації загрози застосовуються два показники: рівень початкової захищеності та частота (імовірність) реалізації даної загрози.

При створенні переліку актуальних загроз безпеки кожного ступеня початкової захищеності ставиться у відповідність чисельний коефіцієнт Y_1 , а саме:

- 0 - для високого ступеня початкової захищеності;
- 5 - для середнього ступеня початкової захищеності;
- 10 - для низького ступеня початкової захищеності.

Під імовірністю реалізації загрози мається на увазі обчислювальний експертним шляхом показник, що характеризує, наскільки імовірно є реалізація конкретної загрози. При обчисленні переліка актуальних загроз безпеки кожної градації імовірності виникнення загрози ставиться у відповідність чисельний коефіцієнт Y_2 , а саме:

- 0 - для малоймовірної загрози;
- 2 - для низької імовірності загрози;

5 - для середньої імовірності загрози;

10 - для високої імовірності загрози.

З урахуванням викладеного, коефіцієнт реалізації загрози Y буде обчислюватись співвідношенням

$$Y = (Y_1 + Y_2) / 20$$

За значенням коефіцієнту реалізації загрози формується вербальна інтерпретація можливості реалізації загрози наступним чином:

Якщо $0 \leq Y \leq 0,3$, то можливість реалізації загрози вважається низькою;

Якщо $0,3 < Y \leq 0,6$, то можливість реалізації загрози вважається середньою;

Якщо $0,6 < Y \leq 0,8$, то можливість реалізації загрози вважається високою;

Якщо $Y > 0,8$, то можливість реалізації загрози вважається дуже високою.

Таблиця 3.4 - Модель загроз

№	Загроза	Y_2	Y	Можливість реалізації загрози	Небезпека	Актуальність
1	Загроза витоку акустичної інформації	0	0,25	низька	низька	неактуальна
2	Загрози витоку візуальної інформації	2	0,35	середня	низька	неактуальна
3	Загрози, направлені на перехоплення паролів, модифікацію базової системи вводу\виводу, перехоплення керування завантаженням	5	0,5	середня	середня	актуальна
4	Загрози виявлення паролів	5	0,5	середня	середня	актуальна

Кінець таблиці 3.4

5	Загрози, направлені на отримання НСД із застосуванням стандартних функцій ОС або будь-якої прикладної програми із застосуванням спеціально створених для отримання НСД програм	5	0,5	середня	висока	актуальна
6	Загроза впровадження шкідливого ПЗ	5	0,5	висока	висока	актуальна
7	Загрози сканування, направленні на виявлення типу ОС, мережевих адрес, робочих станцій, відкритих портів та служб, відкритих з'єднань	10	0,75	висока	висока	актуальна
8	Загрози отримання НСД шляхом заміни довіреного об'єкту	2	0,35	середня	низька	неактуальна
9	Загрози впровадження помилкового об'єкту мережі	2	0,35	середня	низька	неактуальна
10	Загрози віддаленого запуску застосунків	2	0,35	низька	низька	неактуальна
11	Загрози нав'язування хибного маршруту шляхом несанкціонованої зміни маршрутно-адресних даних	2	0,35	низька	низька	неактуальна

3.2 Вимоги до створення КСЗІ

Аудит ІС об'єкта захисту показав, що на підприємстві циркулює інформація, що має високу ступінь важливості. В результаті проведення аудиту ІС підприємства був створений перелік актуальних загроз безпеки. Для створення КСЗІ необхідно передбачити засоби для нейтралізації цих загроз. Ці засоби мають

ґрунтуватись на та не суперечити законам України, федеральним законам, нормативно правовим актам, постановленням та розпорядженням Уряду України. Механізми захисту, які використовуються для побудування захищених систем, повинні бути взаємопов'язані за місцем, часом та характером дії. Комплексність передбачає також використання різноманітних методів та засобів захисту інформації: організаційних, технічних, програмних, криптографічних, правових. Система захисту повинна мати декілька рівнів, що перекривають один одного.

Інженерно-технічні засоби захисту мають бути направлені на запобігання доступу порушників до приміщення офісу, до інформаційної середи ІС та розмежування повноважень користувачів.

Програмно-апаратна система захисту повинна забезпечувати конфіденційність, цілісність та доступність інформації, що опрацьовується.

Організаційні методи захисту інформації включають до себе міри, події та дії, які повинні виконувати повноважні особи у процесі роботи з інформацією для забезпечення заданого рівня безпеки. Елементи організаційного захисту повинні включати до себе не тільки документи, пов'язані з роботою з конфіденційною інформацією, а й документи, що забезпечують організацію захищеного документообігу з учасниками системи електронного документообігу.

3.3 Програмно-апаратний захист комунального підприємства

На об'єкті, що знаходиться під захистом, слід розташувати відеокамери у місцях можливого проникнення злоумисників, а також у місцях, з яких можливо спостерігати за переміщенням відвідувачів по коридору поверху. Камери розташовуються так, щоб під спостереженням знаходились пожежні виходи, ліфти, коридор, входи до будівлі. Також додатково відеокамери розташовуються ззовні на периметрі об'єкту для виключення можливості злоумисників розташувати апаратні закладки ззовні об'єкту. Із запропонованого на ринку вибору телевізійних відеокамер була обрана вулична кольорова відеокамера Samsung SC)-2080RP. Оскільки вона має високе розширення, гарну

світлочутливість та вбудований варіофокальний об'єктив з автофокусом та фокусною відстанню, дана відеокамера повністю задовольняє вимоги щодо кута огляду для всіх зон спостереження всередині та ззовні об'єкта захисту.

Функції поста керування на об'єкті виконує приміщення, розташоване на першому поверсі будівлі. На пості керування цілодобово повинен знаходитись охоронець. На посту керування слід розташувати сервер відеоспостереження з монітором та засіб охоронно-пожежної сигналізації за модулем спостереження та керування.

Для забезпечення надійного захисту даних від загрози впливу шкідливого програмного забезпечення на всіх робочих станціях і сервері підприємства повинні бути встановлені антивірусні пакети з безперервним автоматичним обов'язковим оновленням антивірусних баз з локального дзеркала, розміщеного на сервері.

Призначення антивірусного програмного забезпечення Dr.Web для Windows - забезпечення надійної високоякісної захисту робочих станцій і персонального комп'ютера від вірусів і інших шкідливих програм.

Антивірус Dr.Web для Windows версії є лідером в лікуванні активних заражень. Має високу ймовірність успішного запуску процесу сканування на зараженому ПК - навіть з зовнішнього носія без установки в систему.

Переваги антивірусного програмного забезпечення Dr.Web для Windows:

- ефективний засіб постійного моніторингу здоров'я комп'ютера; перехоплення "на льоту" всіх звернень до файлів на дисках;
- захист конфіденційної інформації - краще в галузі виявлення троянських програм і клавіатурних шпигунів;
- не маюча аналогів технологія самозахисту Dr.Web Self PROtect;
- недосяжна для конкурентів якість виявлення і нейтралізація складних вірусів, таких як MaosBoost, Sector;
- мінімальне навантаження на ресурси ПК і непомітна дія при роботі користувача з іншими додатками;

- захист засобами Dr.Web Shield від вірусів, що використовують rootkit-технології;
- визначення вірусів в архівах будь-якого ступеня вкладеності та в упакованих об'єктах;
- унікальна технологія несигнатурного пошуку Origins.Tracing та інтелектуальний евристичний аналізатор Dr.Web - захист від невідомих загроз;
- захист від масових розсилок вихідної електронної кореспонденції поштовими хробаками.

Антивірус Касперського для Windows Servers - це додаток для захисту файлових серверів під керуванням ОС Windows Server (включаючи x64) від усіх типів шкідливих програм. Рішення розроблено з урахуванням підвищених вимог до серверів для роботи в умовах високих навантажень.

Додаток контролює всі вхідні і вихідні потоки даних на комп'ютері - електронну пошту, інтернет-трафік і мережеві взаємодії. Глибока інтеграція всіх компонентів програми дозволяє уникнути системних конфліктів і забезпечує високу швидкість роботи програми.

Інсталювання програми на робочі станції, налаштування параметрів її роботи, своєчасне оновлення баз сигнатур та програмних модулів, а також оперативне реагування в критичних ситуаціях - всі ці завдання адміністратор мережі може вирішувати віддалено та централізовано, використовуючи консоль керування Kaspersky Administration Kit.

Евристичний аналізатор, що входить до складу Антивірус Касперського, забезпечує захист від нових шкідливих програм ще до того, як їх опис додається в бази сигнатур. Додаток аналізує всі процеси, запущені у системі, своєчасно попереджаючи користувача про небезпеку; в разі необхідності імітує запуск підозрілих програм в ізольованому віртуальному середовищі; дозволяє відновити дані, пошкоджені шкідливим ПЗ.

Нове антивірусне ядро дозволяє регулярно оновлювати його окремі модулі без перевстановлення програми. Завдяки цьому клієнти «Лабораторії

Касперського» завжди мають у своєму розпорядженні найсучасніші методи захисту від нових шкідливих програм.

Однією з важливих задач при експлуатації інформаційних систем є забезпечення цілості даних, тому необхідно мати механізм для швидкого відновлення втрачених даних. Це може бути забезпечено шляхом побудови розвиненої системи резервного копіювання, що періодично створює копії інформації з метою її подальшого відновлення в разі часткового або повного руйнування.

До системи резервного копіювання доцільно пред'явити наступні вимоги:

- використання технології «клієнт-сервер» при реалізації системи мережевого резервного копіювання;
- забезпечення автоматизації робіт резервного копіювання;
- використання адекватного носія резервної копії;
- виконання верифікації та стиснення інформації;
- швидке відновлення серверів мережі після аварії;
- резервне копіювання баз даних прикладних систем в оперативному режимі;
- підтримка гетерогенного середовища;
- розвинені засоби управління і моніторингу.

Даним вимогам задовольняє програмне забезпечення Acronis Backup & Recovery 10 Advanced Server.

Acronis Backup & Recovery 10 Advanced Server - продукт, розроблений для підприємства будь-якого розміру, росте разом з компанією, легко масштабується від локальних конфігурацій до роботи у великих територіально розподілених мережах на тисячі машин. Він надає організаціям розширені можливості резервного копіювання та відновлення системи: дедуплікацію даних, підвищену безпеку, панель моніторингу операцій.

Основні переваги Acronis Backup & Recovery 10 Advanced Server:

- швидке і надійне відновлення;

- процеси резервного копіювання та відновлення усіх робочих станцій та серверів керуються з єдиної централізованої панелі моніторингу, що відображає інформацію про всі виконувані або заплановані завдання;

- дедублікація на рівні файлів та блоків виключає повторне резервне копіювання одних і тих же даних, що істотно скорочує витрати на передачу та зберігання резервних копій;

- групове опрацювання завдань за допомогою політик резервного копіювання та відновлення дозволяє автоматизувати однотипні дії, такі як відновлення багатьох машин в мережі, і не витрачати час на індивідуальний запуск кожного завдання.

Задля запобігання витоку інформації шляхом перехоплення мережевого трафіку слід використовувати технологію IP in IP. IP in IP — це протокол IP-тунелювання, який інкапсулює один IP-пакет в інший IP-пакет. Інкапсуляція одного IP пакета в інший IP пакет, це додавання зовнішнього заголовка з SourceIP — точкою входу в тунель, і Destination — точкою виходу з тунелю. При цьому внутрішній пакет не був змінений (крім поля TTL, який зменшився). Поля "Do not Fragment" і "The Type of Service" повинні бути скопійовані в зовнішній пакет. Якщо розмір пакета більше ніж Path MTU, пакет фрагментується в інкапсуляторі, оскільки зовнішній заголовок має бути включеним. Декапсулятор повинен буде зібрати пакет. Налаштований тунель допомагає зменшити кількість діючих політик IPsec. Оскільки у тунелі відбувається інкапсуляція трафіку то можливо будувати будь-які маршрути, прописуючи лише дві адреси у політиках IPsec. Для підвищення рівню безпеки потрібно використовувати шифрування IPsec. Шифрування дозволяє приховати інформацію, що передається за тунелем, що, в свою чергу, не дозволяє зломиснику прочитати дану інформацію навіть за умови її отримання.

The image shows a configuration window for IPsec. It has two main sections: 'Auth. Algorithms' and 'Encr. Algorithms'. In the 'Auth. Algorithms' section, 'md5' is unchecked, 'sha1' is checked, 'null' is unchecked, 'sha256' is unchecked, and 'sha512' is unchecked. In the 'Encr. Algorithms' section, 'null' is unchecked, 'des' is unchecked, '3des' is unchecked, 'aes-128 cbc' is checked, 'aes-192 cbc' is checked, 'aes-256 cbc' is checked, 'blowfish' is unchecked, 'twofish' is unchecked, 'camellia-128' is unchecked, 'camellia-192' is unchecked, 'camellia-256' is unchecked, 'aes-128 ctr' is unchecked, 'aes-192 ctr' is unchecked, 'aes-256 ctr' is unchecked, 'aes-128 gcm' is unchecked, 'aes-192 gcm' is unchecked, and 'aes-256 gcm' is unchecked. At the bottom, there is a 'Lifetime' field set to '00:30:00' and a 'PFS Group' dropdown menu set to 'modp1024'.

Рисунок 3.1 - Шифрування трафіку в IPsec

3.4 Фізичний захист інформації

До фізичних засобів захисту інформації можна віднести усі засоби, що запобігають фізичному доступу до обладнання з інформацією та доступ до інформації при фізичному знаходженні на захищеному об'єкті.

Насамперед потрібно зазначити вимоги щодо кімнати, у якій проводяться усі наради, на яких обговорюється важлива інформація. Дана кімната повинна бути побудована за принципом клітки Фарадея. Клітка Фарадея (також відома як екран Фарадея) - замкнена у просторі огорожа, сформована з електропровідного матеріалу (у вигляді суцільних елементів або сітки). Така огорожа нейтралізує зовнішні статичні та динамічні електричні поля в середині себе. Прийом або передача радіохвиль за допомогою антени, розміщеної в клітці Фарадея, стає практично не можливою. Сигнал значно послаблюється або взагалі повністю блокується кліткою. При створенні кліток Фарадея можуть бути застосовані різноманітні типи матеріалів, до яких можна віднести:

- листові металічні екрани;
- фольгові матеріали;
- спеціальні тканини;
- електропровідні клеї;
- електропровідні фарби;
- сіткові матеріали;

Стінки кімнати, у якій відбуваються наради, повинні бути подвійними з обов'язковою повітряною прослойкою між стінами. Дане рішення знеможливило отримання інформації шляхом застосування спеціальних пристроїв, що зчитують вібрації та переводять їх у текстову інформацію.

Дещо послаблені, але все-такі серйозні заходи повинні бути проведені на по всій території об'єкту, що захищається. На всіх вікнах повинні бути встановлені решітки, що запобігає проникненню зломисників на територію об'єкту скрізь вікна. На вікнах також валиво встановити спеціальні пристрої, що створюють вібрацію задля запобігання дистанційного отримання важливої інформації зломисником шляхом використання спеціального технічного обладнання. Під час покидання працівниками об'єкту усі вікна повинні бути зачиненими для запобігання можливості зломисників підкинути звукозаписуючий пристрій з можливістю дистанційної передачі інформації.

Усі сервери повинні бути розташовані у спеціально обладнаних кімнатах з обмеженим доступом. На даний момент вже існують пристрої, що спроможні зчитати інформацію з серверів, аналізуючи звук роботи вентилятора, що забезпечує охолодження серверів. Це означає, що кімнату потрібно будувати з оглядом на можливість отримання зломисником доступу до охолоджуючого вентилятора. У даній кімнаті повинні розташовуватись усі сервери, включаючи сервери з резервними копіями інформації. Допускається залишити тестовий сервер, на якому будуть проходити тестування нових методів програмного захисту інформації.

3.5 Організаційний захист інформації

Організаційний захист інформації - це комплекс напрямків і методів керувального, обмежувального та технологічного характеру, що визначають основи і зміст системи захисту, що спонукають персонал дотримуватися правил захисту конфіденційної інформації.

Організаційні методи є стрижнем комплексної системи захисту підприємства. Тільки за допомогою цих методів можливе об'єднання всіх засобів захисту в єдину систему.

До основних організаційних заходів із захисту інформації на об'єкті можна віднести:

- організацію режиму та охорони, яка складається зі створення структури служби безпеки; організацію внутрішньооб'єктного режиму та охорони об'єктів підприємства;
- організацію роботи з персоналом, яка передбачає підбір та підготовку персоналу, перевірку персоналу на благонадійність, укладання контрактів та угод зі співробітниками, навчання правилам роботи з конфіденційною інформацією, ознайомлення із заходами відповідальності за порушення правил захисту інформації;
- організацію роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання та знищення;
- організацію роботи з електронними документами та інформаційною системою підприємства, включаючи роботу в локальній обчислювальній мережі і правила доступу до мережі Інтернет;
- організацію систематичного контролю роботи персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв;

- організацію роботи з відвідувачами, при проведенні нарад і переговорів;
- організацію інформаційно-аналітичної роботи, що складається з аналізу і накопичення інформації з елементами прогнозування з питань, що належать до безпеки керування, і підготовки рекомендацій керівництву щодо правомірного захисту.

До організаційних методів захисту інформації потрібно також віднести розмежування доступу до інформації. Наразі доступ має кожній системний адміністратор. У зв'язку з даним фактом, виникає ризик отримання НСД до ІзОД шляхом отримання доступу до робочого місця одного з системних адміністраторів. Для запобігання даної загрози потрібно дозволити лише одній людині у відділі мати доступ до інформації та максимально захистити її робочу станцію.

Також слід кожен місяць проводити заходи, метою яких є пошук програмно-апаратних закладних пристроїв. В останні роки все більша кількість атак є комплексними, тобто з використанням різноманітних програм та пристроїв. Підготовка до такої атаки може зайняти від двох місяців до півроку, отже, потрібно кожен місяць проводити пошук признаков атаки, що планується, та знешкоджувати усі виявлені пристрої та програми, виявлені у ході пошуку.

Висновки щодо розділу 3

У данному розділі мною були розглянуті питання, які виносяться на аудит. Був розглянутий та досліджений перелік ІзОД, створена таблиця з розподіленням певної інформації по категоріям та ступеням конфіденційності. Також розглянуті загрози безпеці інформації, створена таблиця з розподіленням ризиків та вразливостей. Був проведений аналіз загроз та запропоновані методи запобігання. Окремо був розглянутий коефіцієнт ймовірності реалізації загрози та власна модель загроз для комунального підприємства; актуальність відомих загроз. Були виділені вимоги щодо побудування КСЗІ. Були запропоновані

апаратні та програмні засоби захисту інформації та рекомендації щодо їх експлуатації. Також у даному розділі були запропоновані варіанти посилення захисту об'єкту за допомогою фізичних та програмних засобів.

ВИСНОВКИ

В даній роботі було зроблено загальний огляд КСЗІ, проблем, що вона вирішує та методів створення КСЗІ на підприємстві.

В ході виконання бакалаврської роботи були досліджені:

1. Існуючі рішення КСЗІ. Були детально розглянуті комплексні системи захисту інформації “Панцир+”, “Secret Net Studio”, СЗІ ВІ “Dallas Lock”. Були досліджені можливості наведених прикладів існуючих комплексних систем захисту інформації, розглянуті їх функції та вимоги. Детально були розглянуті компоненти, наявні у наведених КСЗІ. Не слід забувати, що є можливість покращувати КСЗІ, додаючи до неї різноманітні ПАК, інсталиючи різноманітні додаткові програми, такі як системи IDS та IPS, додавати технічне забезпечення, таке як сервери та мережеві екрани.

2. Послідовність етапів створення етапів КСЗІ, питання, документи що розглядаються та створюються на кожному з етапів. Було розглянуто створення політики безпеки підприємства та елементи, які вона повинна до себе включати. Були наведені документи та норми, яким повинна відповідати КСЗІ. Якщо КСЗІ не відповідає хоч одній нормі то компанія чи підприємство не зможе отримати атестат, а отже, ІС даної компанії чи підприємства неможливо вважати захищеною.

3. Питання аудиту, необхідність створення КСЗІ на даному підприємстві, ступені конфіденційності циркулюючих на даному підприємстві даних та документів. Були визначені області захисту, ризики та загрози, які можуть призвести до отримання НСД до ІзОД, крадіжок інформації, втрат внаслідок стихійних лих. Була створена особиста таблиця ризиків, запропоновані методи їх запобігання. Додатково була створена таблиця актуальності питань захисту певних шляхів втрати чи отримання НСД до ІзОД. Були надані рекомендації щодо апаратного та програмного забезпечення для реалізації КСЗІ на даному підприємстві.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Опис КСЗІ “Панцир+”[Електронний ресурс]. Режим доступу:
<https://www.anti-malware.ru/products/kszi-pancir-plus>
2. Опис КСЗІ “Secret Net Studio”[Електронний ресурс]. Режим доступу:
<https://www.anti-malware.ru/products/secret-net-studio>
3. Опис СЗІ ВІ “Dallas Lock”[Електронний ресурс]. Режим доступу:
https://www.anti-malware.ru/products/Dallas_Lock
4. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Режим доступу:
https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf?fbclid=IwAR16Qka92G63wtjvFfHcK5rALmf2z0iKjdO0rN6f005_fxovlJX3-Rtlpqk
5. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Режим доступу:
<https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf>
6. Гребенніков В.В. - Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій. 2013. 161 с. - Режим доступу:
<https://mybook.ru/author/vadimgrebennikov-3/kompleksni-sistemi-zahistuinformaciyi-proektuvann/>
7. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Режим доступу:
<https://tzi.com.ua/downloads/3.7-003-2005.pdf?fbclid=IwAR078jEedTuTzkNMfZlybcuywbBxCJr1znhTvkKEpYywIPP3FRBZGqAr3AI>

8. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет[Електронний ресурс]. Режим доступу:

https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennnya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet?fbclid=IwAR3RcWOpttuJROqWpz0bwL1u-0OsySollvFJqw2vLCFk6X_EA79Se3_1ZY

9. Б74 Інформаційна безпека держави. — К.: “МК-Прес”, 2005. — 432с., іл. 1. Режим доступу:

<https://studfile.net/preview/5375874/>

10. Юдін О.К. Правові аспекти формування системи державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Безпека інформації - 2014. - Том 20 (1) / Технічні науки. - С. 76-82.

11. Положення про Єдину автоматизовану інформаційну систему Державної митної служби України (затверджено наказом Державної митної служби України від 04.11.2010 № 1341). - [Електронний ресурс]. - Режим доступу:

<http://sfs.gov.ua/data/normativ/000/000/62603/2.doc>.

12. Юдін О.К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О.К. Юдін, С.С. Бучик, А.В. Чунарьова, О.І. Варченко // Наукоємні технології - 2014. № 2(22) / Технічні науки. - С. 200-210.