НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

Факультет транспортних та інформаційних технологій

Кафедра інформаційно-аналітичної діяльності та інформаційної безпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра

на тему:

«Проектування та розробка системи захисту інформації»

Виконав: студент IV курсу, групи ІБК-IV-1
Спеціальність «Комп'ютерні науки»
Освітньо-професійна програма «Інформаційна безпека в комп'ютеризованих системах»

_____ Ю.Р. Орел
(підпис) (Ініціали Прізвище здобувача освіти)

Керівник: к.т.н., доц. _____ М.М. Дехтяр
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Нормоконтроль: доктор філософії, ас. _____ А.Є. Клочан
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Допущений до захисту
«___»_____20__р.

Завідувач кафедри: д.т.н.,проф. _____ А.Н. Аль-Аморі
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Рецензент: к.т.н., доц. _____ В.В. Сватко
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Київ – 2024

НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

Факультет транспортних та інформаційних технологій

Кафедра інформаційно-аналітичної діяльності та інформаційної безпеки

Рівень вищої освіти: перший (бакалаврський)
Спеціальність 122 Комп'ютерні науки

Освітня програма «Інформаційна безпека в комп’ютеризованих системах»

ЗАТВЕРДЖУЮ

Завідувач кафедри ІАДІБ

_____ А.Н.Аль-Амморі

“_” _____20___р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ

Орлу Юрію Романовичу

(прізвище, ім’я та по-батькові студента)

1. Тема роботи: «Проектування та розробка системи захисту інформації»
керівник роботи: Дехтяр Марина Михайлівна к.т.н., доц.

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Національного транспортного університету від «18» березня 2024 року № 94

2. Строк подання студентом роботи 21.06.2024 р.
3. Вихідні дані до роботи: Існуючі продукти комплексних систем захисту інформації, існуючі методи та етапи створення комплексних систем захисту інформації, існуючих систем захисту інформації на підприємстві.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

1. Проаналізувати сфери інформації які повинні захищати КСЗІ.
2. Дослідити наявні засоби КСЗІ.

3. Розробити алгоритм створення комплексної системи захисту інформації на прикладі ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС».

4. Запропонувати покращення та вдосконалити систему захисту інформації ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС», виявивши наявні недоліки та розробити способи зниження імовірності атаки на підприємство.

5. Перелік ілюстративного матеріалу/слайдів презентації (з точним зазначенням обов'язкових ілюстрацій):

1) Організаційні заходи до побудови КСЗІ.
2) Розглянуті комплексні системи захисту інформації.
3) Недоліки системи захисту інформації ТОВ «ААЗ Трейдінг-Автолюкс».
4) Аналіз вразливостей на ТОВ «ААЗ Трейдінг-Автолюкс» та способи їх уникнення.
5) Актуальність загроз.
6) Запропонований програмно-апаратний захист підприємства.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання: 18 березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ
БАКАЛАВРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
по кафедрі інформаційно-аналітичної діяльності та інформаційної безпеки
(для студентів денної форми навчання)

№ етапу	Найменування етапу	Дата виконання	Примітка
1	Отримання завдання	18.03.2024	Виконано
2	Аналіз літературних джерел	18.03-01.04.2024	Виконано
3	Підготовка та написання 1-го спеціального розділу	01.04-08.04.2024	Виконано
4	Підготовка та написання 2-го спеціального розділу	09.04-16.04.2024	Виконано
5	Підготовка та написання 3-го спеціального розділу	17.04-05.05.2024	Виконано
6	Перший попередній захист	06.05.2024 р.	Виконано
7	Написання висновків та переліку посилань	07.05.2024-01.06	Виконано
8	Оформлення дипломної роботи і графічного матеріалу	03.06-10.06.2024	Виконано
9	Другий попередній захист	11.06.2024	Виконано
10	Перевірка роботи на плагіат та підготовка документів до захисту	17.06-19.06.2024	Виконано
11	Здача закінченої роботи	21.06.2024	Виконано
12	Захист	25.06.2024	Виконано

Здобувач освіти _____ Ю.Р. Орел
(підпис) (Ініціали Прізвище)

Керівник роботи,

к .т.н., доц _____ М.М. Дехтяр
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API - application programming interface;

BYOD - bring your own device;

CASB - cloud access security broker;

DevOps – development operations;

DI – digital innovation;

DLP - data loss prevention;

EDR - endpoint detection and response;

GIN - generalized inverted index;

ICA - information centric analytics;

ICD - integrated cyber defense;

ICDx - integrated cyber defense exchange;

MaaS - metal-as-a-service;

ML - machine learning;

NAC - network access control;

NGFW - next-generation firewall;

RBAC - role-based access control;

REST - representational state transfer;

SaaS - software as a service;

SASE - secure access service edge;

SEP - symantec endpoint protection;

SESC - symantec endpoint security complete;

SOAR - security orchestration, automation, and response;

SOC - security operations center;

SPU - special processing unit;

SSL - secure sockets layer;

SSO - single sign-on;

SWG - secure web gateway;

TLS - transport layer security;

URL - uniform resource locator;

VPN - virtual private network;

WAF - web application firewall;

WSS - web security service;

БД - база даних;

ВІ - віртуальна інфраструктура;

ЕОМ - електронно-обчислювальна машина;

ІзОД - інформація з обмеженим доступом;

ІТС - інформаційно-телекомунікаційна система;

КЗЗ - комплекс засобів захисту від несанкціонованого доступу;

КС - комп'ютерна система;

КСЗІ - комплексна система захисту інформації;

НД - нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НДМ - недекларовані можливості;

НДР - науково-дослідна робота;

НСД - несанкціонований доступ;

ОС - операційна система;

ОТЗ - основні технічні засоби;

ПАК - програмно-апаратний комплекс;

ПЕМВН - побічні електромагнітні випромінювання та наведення;

ПЕОМ - персональна електронно-обчислювальна машина;

ПЗ - програмне забезпечення;

СБ - сервер безпеки;

СЗІ - служба захисту інформації;

СУІБ - система управління інформаційною безпекою;

ТЗ - технічне завдання;

ТЗІ - технічний захист інформації.

ЗМІСТ

ВСТУП

Прийняття рішень у всіх сферах діяльності підприємства або організації стає все більш залежним від інформаційних процесів. Аналіз цих процесів та формування управлінських рішень здійснюються на основі інформаційних моделей, побудованих з використанням сучасних інформаційно-телекомунікаційних технологій. В цьому контексті захист інформації стає ключовим аспектом безпеки підприємства, чиє значення зростає щороку.

Інформаційні ресурси стають найважливішим джерелом економічної ефективності для підприємств. Вся сфера її діяльності має тенденцію залежати від розвитку інформаційних технологій, і в цьому процесі вона не тільки створює, але й споживає інформацію.

Таким чином, наростає потреба у створенні комплексних систем захисту інформації на підприємствах, а також у підготовці фахівців цієї галузі.

Метою бакалаврської кваліфікаційної роботи є вивчення та аналіз існуючих систем захисту інформації, включаючи технічні та програмні засоби захисту інформації, а також розробка пропозицій щодо їх вдосконалення по відношенню до існуючих систем захисту інформації з метою підвищення рівня безпеки на підприємстві.

Об’єктом дослідження є процес визначення недоліків захисту інформації на ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС».

Предметом дослідження – є моделі, інструменти, методики та методи створення комплексних систем захисту інформації (КСЗІ) на підприємстві для захисту інформації.

Для досягнення мети в бакалаврській кваліфікаційній роботі вирішено такі завдання:

1. Проаналізувати сфери інформації які повинні захищати КСЗІ.
2. Дослідити наявні засоби КСЗІ.

3. Розробити алгоритм створення комплексної системи захисту інформації на прикладі ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС».

4. Запропонувати покращення та вдосконалити систему захисту інформації ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС», виявивши наявні недоліки та розробити способи зниження імовірності атаки на підприємство.

Ключові слова: КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЗАГРОЗА, КІБЕРАТАКА, ЗАХИСТ ВІД АТАК, БЕЗПЕКА.

РОЗДІЛ 1 АНАЛІЗ ІСНУЮЧИХ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Комплексні системи захисту інформації

Враховуючи вимоги чинного законодавства України та деяких нормативних документів Закону України "Про захист інформації в інформаційно-комунікаційних системах" та Закону України "Про захист персональних даних", обов'язковому захисту підлягає наступна інформація: інформація, що є власністю держави або інформація з обмеженим доступом вимоги щодо захисту якої встановлені законом, у тому числі персональні дані громадян.

Комплексна система захисту інформації (КСЗІ) - це комплекс організаційних, інженерних і технічних заходів, спрямованих на захист інформації від модернізації, витоку, розголошення та несанкціонованого доступу. Організаційні заходи стають найважливішим і найпотрібнішим елементом побудови комплексних систем захисту. Інженерні та технічні заходи реалізуються в міру необхідності.

Організаційні заходи містять розробку задум інформаційної безпеки, в тому числі:

- розробка посадової інструкції для юзерів та персоналу, що обслуговує;
- розробка правил управління елементами обліку, тиражування, інформаційної системи, зберігання, тиражування та знищення носіїв інформації та ідентифікації користувачів;
- розробка плану дій на випадок НСД до інформаційних ресурсів системи, втрачання працездатності засобів захисту або виявлення надзвичайної ситуації;

- підготовка та навчання користувачів положенням інформаційної безпеки.

За потреби, в межах організаційних заходів може створюється служба безпеки інформації, а також реорганізована система управління та збереження документованої інформації.

Технічні та інженерні заходи які стосуються захищеності інформаційної інфраструктури підприємства включають безпечні з'єднання, брандмауери, розділення інформаційних потоків між частинами мережі, шифрування та захист від доступу до інформації сторонніх осіб.

За потреби в межах інженерно-технічних заходів на об'єкті встановлюються системи безпеки, пожежної сигналізації, контролю доступу та управління.

Деякі приміщення обладнані для запобігання витоку акустичної (звукової) інформації.

У процесі розробки КСЗІ повинні залучатися такі сторони:

- організація, яка має потребу в побудові КСЗІ (Замовник);
- організація, яка виконує весь спектр потрібних дій для побудови КСЗІ для іншої організації (Виконавець);
- Адміністрація Державної служби спеціального зв’язку та захисту інформації України (Орган контролю);
- організація, яка проводить державну експертизу КСЗІ;
- організація, яка при потребі залучається організацією-замовником або організацією-виконавцем задля здійснення деякого роду робіт для розробки КСЗІ (Підрядник).

Предмет захисту комплексної системи захисту інформації це інформаційні дані в усіх їх формах. Матеріальним носієм інформації є сигнал.

За своїми фізичними властивостями інформаційні сигнали поділяються на акустичні, електромагнітні, електричні та їхню сукупність. Сигнали виражаються у вигляді електромагнітних, механічних або інших коливань, а інформація, яка захищається, перебуває в їх змінних. В залежності від свого походження, інформаційні сигнали розповсюджуються у певному фізичному середовищі. Середовище може варіюватися між газами, рідинами і твердими тілами. Прикладами можуть бути повітряний простір, будівельні конструкції, лінії зв'язку, струмопровідні елементи і заземлення.

Залежно від типу і формату інформаційних сигналів, що циркулюють в інформаційно-комунікаційній системі (ІТС), в тому числі всередині автоматизованих системах (АС), для створення КСЗІ використовуються різноманітні засоби та способи захисту.

1.2 Огляд існуючих комплексних систем захисту інформації

На сьогоднішній день більшість компаній надають перевагу Системам Управління Інформаційною Безпекою (СУІБ) перед комплексними системами захисту інформації, оскільки отримати сертифікат відповідності ISO/IEC 27001 є більш простим. Не потрібно реалізовувати всі технології захисту одразу, достатньо лише обіцяти реалізувати їх до кінця року. Однак складність створення інтегрованої системи інформаційної безпеки (ІСІ) полягає також у необхідності створення інфраструктури в Україні. У такому контексті, вони спрямовані на відміну стандарту КСЗІ та перехід до СУІБ.

У цьому дослідженні розглядаються три існуючі інтегровані системи захисту інформації. Оскільки на ринку існує велика кількість готових СУІБ, буде проаналізовано три з них.

1.2.1 Symantec Integrated Cyber Defense (ICD)

Symantec Integrated Cyber Defense (ICD) - це комплексна платформа кібербезпеки, розроблена компанією Broadcom Inc.**,** після придбання Symantec Enterprise Security у 2019 році.

Symantec Integrated Cyber Defense була спочатку розроблена компанією Symantec Corporation, провідною компанією у сфері кібербезпеки. У 2019 році Symantec Enterprise Security була придбана компанією Broadcom Inc., яка продовжує розвиток та підтримку цієї платформи.[11]

Symantec Integrated Cyber Defense призначена для забезпечення всебічного захисту інформаційних активів організацій. Вона ефективна як проти точкових, так і проти комплексних кіберзагроз.

Основна мета Symantec Integrated Cyber Defense - забезпечити повний та найефективніший захист активів організацій.

Оскільки організації впроваджують цифрову трансформацію та розглядають принцип нульової довіри або створення архітектури Secure Access Service Edge (SASE), існує велика привабливість у використанні інтегрованого підходу до кіберзахисту. Symantec™ Integrated Cyber Defense об'єднує продукти, послуги та партнерів, щоб знизити вартість і складність кібербезпеки, одночасно захищаючи підприємства від складних загроз. Поєднуються найкращі у своєму класі засоби захисту інформації, захисту від загроз, керування ідентифікаційними даними, дотримання нормативних вимог та інші передові послуги, що базуються на спільному інтелекті та автоматизації між кінцевими точками, мережами, програмами та хмарними точками керування програмами.

Інтегруючи кілька продуктів безпеки в єдину систему, Symantec Integrated Cyber Defense покращує виявлення, координуючи висновки окремих продуктів

для виявлення і блокування подій, які в іншому випадку могли б залишитися непоміченими.

Організації також повинні мати можливість зберігати та отримувати дані з різних місць. З організаційними даними слід поводитися інакше, ніж з даними, які не належать до них. Організації повинні встановлювати належні правила доступу, вирішувати, де зберігається інформація, і враховувати міркування конфіденційності. Symantec Integrated Cyber Defense пропонує спосіб нормальної та централізованої обробки даних, що дозволяє фільтрувати поля, типи подій та пересилати їх до потрібних пунктів призначення.

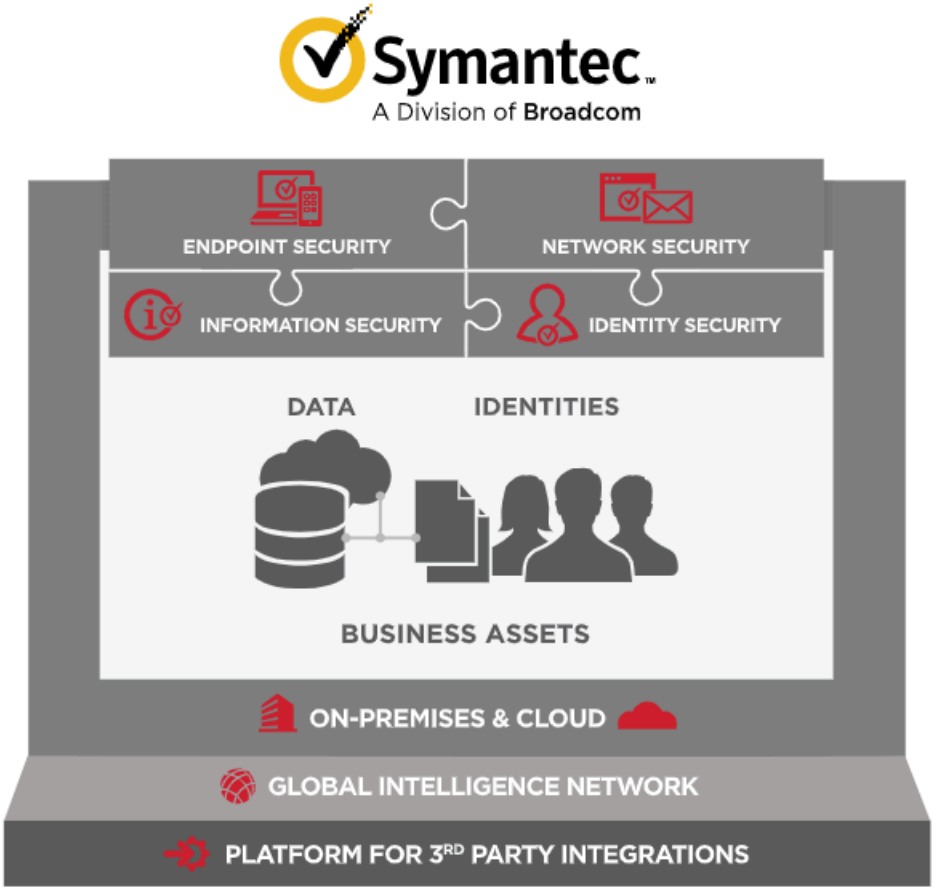

Рисунок 1.1 — Інтегрований кіберзахист Symantec

Завдяки здатності об'єднувати локальні та хмарні середовища, використовувати глибоку розвідку загроз та інтегрувати сторонні технології,

рішення Symantec мають унікальні можливості для того, щоб надати організаціям можливість знизити вартість та складність кібербезпеки та отримати більше користі від існуючих інвестицій у технології кібербезпеки.

Symantec, підрозділ Broadcom, має перше і єдине рішення, яке об'єднує і координує функції безпеки як в хмарних, так і в локальних системах. Підприємства можуть використовувати хмару так, як це їм доцільно, не жертвуючи минулими інвестиціями та залежністю від критично важливої інфраструктури.

Прискорення ініціатив цифрової трансформації впливає на кібербезпеку в організаціях і змушує керівників служб безпеки змінити підхід до кібербезпеки та ризиків. На тлі стагнації бюджетів і незадоволених рад директорів керівники служб безпеки повинні не тільки модернізувати свій підхід до кібербезпеки та ризиків, але й продовжувати захищати інвестиції в існуючий стек безпеки.

Symantec Integrated Cyber Defense забезпечує відкриту екосистему, яка дозволяє легко інтегрувати продукти сторонніх виробників і обмінюватися розвідданими за допомогою багатого набору відкритих інтерфейсів прикладного програмування (API). Понад 120 сертифікованих технологічних партнерів створюють найширшу екосистему кібербезпеки, забезпечуючи скоординований і найкращий у своєму класі підхід до захисту, виявлення та реагування на загрози в кінцевих точках, мережах, електронній пошті та хмарних додатках організації.

Symantec Integrated Cyber Defense підкріплюється Глобальною розвідувальною мережею (GIN), яка співвідносить дані з наступних джерел:

- 175 000 000 кінцевих точок;
- 80 000 000 веб-проксі;
- понад 126 000 000 датчиків атаки;
- більше 25 000 вразливостей;

• понад 500 експертів з безпеки в семи глобальних центрах по всьому світу.

Застосовуючи штучний інтелект для аналізу понад дев'яти петабайт даних про загрози безпеці, пропонується найширший і найглибший набір інформації про загрози в галузі. Крім того, це програмне рішення щодня автоматично оновлює свою інформацію про мільйони шкідливих файлів та індикатори загроз URL-адрес. Від кінцевих точок до серверів і на рівні мережевого трафіку, Symantec Integrated Cyber Defense ділиться телеметрією, накопиченою від клієнтів Symantec по всьому світу, створюючи більш глибокий рівень захисту, з яким не може зрівнятися жодна інша компанія.

Рисунок 1.2 — Інтегрована екосистема кіберзахисту Symantec

Symantec Global Intelligence виявила атаки програм-вимагачів WastedLocker. Evil Corp – це не просто вигадана компанія в серіалі. Це реальне складне кіберзлочинне угруповання, яке продовжує не зупинятися перед звинуваченнями ФБР проти своїх лідерів. У червні 2020 року Evil Corp запустила цілеспрямовану атаку програм-вимагачів під назвою WastedLocker проти деяких найбільших компаній США. Ця атака могла легко вибити їх усіх. Мета атак полягала в тому, щоб завдати шкоди IT-інфраструктурі жертви,

зашифрувавши більшість її комп'ютерів і серверів, щоб вимагати багатомільйонний викуп.

Початкова компрометація включала фреймворк SocGholish, який був доставлений жертві в заархівованому файлі JavaScript, що маскується під оновлення браузера через скомпрометовані законні веб-сайти. Другий файл JavaScript профілював комп'ютер за допомогою таких команд, як whoami, net user і net group. Потім він використовував PowerShell для завантаження додаткових сценаріїв PowerShell, пов'язаних із виявленням. Після того, як зловмисники отримали доступ до мережі жертви, вони використовували Cobalt Strike у тандемі з низкою інструментів для викрадення облікових даних, підвищення привілеїв і переміщення мережею для розгортання програми-вимагача WastedLocker на кількох комп'ютерах.

Атаки були завчасно виявлені в ряді клієнтських мереж за допомогою власної цільової хмарної аналітики. Хмарна аналітика цілеспрямованих атак має можливість швидко аналізувати дані з GIN і перетворювати ці дані в більш значущу, дієву аналітику безпеки. Запитуючи сукупність даних, зібраних за всіма категоріями загроз, аналітичний механізм надає інформацію про повний обсяг навіть найскладніших кампаній із загрозами. Команда Threat Hunter переглянула та перевірила активність і швидко зрозуміла, що вона тісно пов'язана з публічно задокументованою активністю, яка спостерігалася на ранніх стадіях атак WastedLocker.

Це відкриття дозволило команді Threat Hunter ідентифікувати додаткові організації, які стали мішенню WastedLocker, і визначити додаткові інструменти, тактики та процедури, які використовували зловмисники. Ця інформація дозволила аналітикам Symantec посилити захист Symantec від усіх етапів атаки. Одночасно команда Threat Hunter надала ранні попередження 68 клієнтам. Завдяки проактивному зв'язку по телефону та електронній пошті, команда успішно забезпечила зрив атак.

Завдяки розподіленим робочим командам підвищена увага приділяється захисту всіх точок атаки. Це види діяльності, які окремі продукти просто не зможуть повторити. Щоб забезпечити найбільш повний і ефективний захист активів в галузі, Symantec Integrated Cyber Defense забезпечує безпеку кінцевих точок, мережеву безпеку (Інтернет і електронна пошта), інформаційну безпеку та безпеку ідентифікації в локальних і хмарних інфраструктурах.

1. Symantec Endpoint Security. Хмара трансформувала бізнес і зробила звичним для співробітників віддалений доступ до даних і додатків з мільярдів пристроїв. Тепер люди працюють з будь-якого місця, і BYOD додав мільярди пристроїв до корпоративної екосистеми.

Сьогодні захист кінцевих точок має враховувати пристрої, програми та мережі. Проблема полягає в тому, що безфайлові програми, програми-вимагачі та інші нові загрози проникають у старі засоби захисту. Приховані атаки та життя за межами землі важче виявити, ніж шкідливе програмне забезпечення, а велика кількість операційних систем для кінцевих точок створює додаткову складність безпеки.

Symantec Endpoint Security є критично важливою лінією захисту для запобігання використанню пристроїв в рамках кібератаки і запобігання потраплянню конфіденційної інформації, що зберігається на цих пристроях, в чужі руки. Як локальне, гібридне або хмарне рішення, Endpoint Security використовує функції зменшення поверхні атаки, запобігання атакам, запобігання порушенням, а також можливості виявлення та реагування для захисту традиційних і мобільних кінцевих пристроїв.

На додаток до функціоналу Endpoint Security, GIN відіграє важливу роль у захисті кінцевих точок. Складна аналітика загроз допомагає командам безпеки краще оцінювати ризики, оптимізувати рішення щодо безпеки та вживати належних заходів для протидії неминучим загрозам. GIN також застосовує широкий спектр машинного навчання, розширену аналітику та

штучний інтелект, щоб допомогти виявити загрози та ініціювати реагування — чи то за допомогою автоматизації, чи то за допомогою аналітика Security Operations Center (SOC).

Модулі Symantec Endpoint Security включають:

• безпека кінцевих точок;

• безпека сервера;

• захист сховища;

• управління кінцевими точками.

2. Symantec Network Security. Традиційний мережевий периметр зник, користувачі є скрізь, і їм потрібен швидкий доступ до даних і хмарних додатків цілодобово. Електронна пошта та Інтернет є джерелом життєвої сили та важливими засобами комунікації майже для кожної сучасної організації. Вони також є основними векторами, які використовуються під час кібератак, тому їх безпека має важливе значення для зниження ризиків безпеки та підтримки безперервності бізнесу. Проблема полягає в тому, що сліпі зони від зашифрованого трафіку створюють вразливості, кількість цільових фішингових атак зростає, а сучасні загрози перевантажують застарілий захист мережі.

У хмарі, локально або в обох випадках вам потрібно зупинити вхідні та вихідні загрози, націлені на кінцевих користувачів, інформацію та ключову інфраструктуру. Сучасний захист Інтернету та електронної пошти має враховувати цю нову реальність, балансуючи між безпекою, продуктивністю, складністю та вартістю.

Symantec Network Security забезпечує швидкий, безпечний і сумісний доступ до корпоративних даних через сучасні робочі процеси в Інтернеті та електронній пошті. Network Security забезпечує безшовну інтеграцію технологій безпеки в Інтернеті та електронній пошті. Він охоплює кінцеві точки, хмару, мережу та вектори електронної пошти; розширений захист від загроз, ізоляція та управління зашифрованим трафіком; а також виявлення

загроз електронною поштою та реагування на них із широкими можливостями видимості та виправлення.

Модулі Symantec Network Security включають:

• безпечний веб-шлюз;

• веб-ізоляція;

• безпечний поштовий шлюз;

• контент-аналіз за допомогою пісочниці;

• криміналістика та управління зашифрованим трафіком;

• доступ до мережі з нульовою довірою.

3. Symantec Information Security. Дуже важливо, захистити свою організацію від витоку даних і викрадення. Порібно розуміти, як конфіденційні дані передаються між користувачами, пристроями та мережами. Необхідно знати, коли дані піддаються найбільшому ризику викриття, і переконатися, що вони не потраплять у чужі руки. Однак команди безпеки стикаються з безпрецедентними проблемами, коли справа доходить до управління та захисту даних. Вони захищають все більш розмитий периметр мережі та розширені поверхні атак, вирішують безліч нормативних вимог і вимог відповідності, а також прискорюють перехід від застарілих до гібридних хмарних середовищ.

У моделі нульової довіри, коли неможна довіряти будь-чому у своїй мережі або поза нею, фокусування периметра навколо даних і захист їх за допомогою інтелектуальної автентифікації є найкращим підходом до безпеки. Більшість рішень для автентифікації на ринку автентифікують доступ майже до всього, крім ваших даних. Щоб успішно впровадити нульову довіру, потрібна видимість того, хто отримує доступ до ваших даних як локально, так і в хмарі. Перш ніж користувачеві буде надано доступ, необхідно оцінити всі фактори ризику, пов'язані з користувачем та його пристроєм автентифікації.

Архітектури мережевої безпеки, які ставлять корпоративний центр обробки даних у центр вимог до підключення, перешкоджають вимогам до

динамічного доступу цифрового бізнесу. Альтернативою є об'єднання мережевих можливостей і можливостей Software as a Service (SaaS) в SASE, щоб політики безпеки були пов'язані з перевіркою ідентичностей, а не з захистом IP-адрес, і ідентичності більше не базувалися на розташуванні.

Symantec Information Security забезпечує повну видимість і контроль над даними, що протікають у вашій організації, за допомогою тісно інтегрованого рішення, яке бездоганно працює для зміцнення позиції безпеки і можливостей нульової довіри. Інформаційна безпека встановлює стандарт захисту даних за допомогою найкращих у своєму класі інструментів, які можуть захистити ваші дані на кінцевій точці, у мережах і в хмарі, визначити поведінку з високим ризиком, щоб можливо було зупинити внутрішні загрози, а також дозволити віддаленим співробітникам, які мають доступ до корпоративних ресурсів і даних, працювати безпечно та продуктивно.

Модулі інформаційної безпеки Symantec включають:

• запобігання втраті даних;

• CloudSOC CASB;

• інформаційно-центрична аналітика.

4. Symantec Identity Security. Бізнесом рухає необхідність швидкого запуску нових додатків і сервісів, щоб підключати клієнтів і співробітників до послуг в будь-якому місці і в будь-який час. Проблема полягає в тому, що користувачі та програми є основною точкою атаки з боку кіберзлочинців, які сподіваються використати їхній доступ і привілеї та завдати шкоди. Щоб захистити бізнес, потрібно забезпечити безпечний доступ до авторизованих ресурсів, запобігти випадковому витоку даних, захиститися від неправомірного використання облікових даних та облікових записів, а також захистити конфіденційність користувачів.

Symantec Identity Security знижує ці ризики безпеки, застосовуючи детальні політики безпеки, щоб зупинити несанкціонований доступ до

конфіденційних ресурсів і даних, забезпечуючи при цьому безперешкодний доступ довіреним користувачам. Identity Security використовує аналітику GIN і розширену аналітику у всіх продуктах для аналізу активності на кінцевих точках і впевненого визначення легітимності людських і нелюдських ідентичностей.

Модулі Symantec Identity Security включають:

• автентифікацію;

• управління доступом;

• управління привілейованим доступом;

• управління ідентифікацією.

Кожне нове порушення є ще одним нагадуванням про те, що жодна технологія не зможе належним чином захистити підприємство від усіх ризиків кібербезпеки. Symantec Integrated Cyber Defense відповідає на цю проблему таким чином, що відрізняє її від застарілих підходів до безпеки, забезпечуючи інтеграцію на рівні продукту, між продуктами Symantec і по всьому стеку безпеки, включаючи системи сторонніх виробників.

1. Інтеграція на рівні продукту

На рівні продукту Symantec Integrated Cyber Defense знижує складність за рахунок інтеграції раніше автономних рішень в єдині, когерентні продукти. Одним із прикладів є Symantec Endpoint Security Complete (SESC), який об'єднує Symantec Endpoint Protection (SEP), Symantec Endpoint Detection and Response (EDR), Threat Detection Active Directory та Mobile Security в одному продукті, щоб забезпечити зменшення поверхні перед атакою, запобігання атакам, запобігання порушенням, а також реагування та виправлення. Клієнтам достатньо встановити лише одного агента, який виконує всі необхідні завдання. Такий тип інтеграції має більшу цінність для клієнтів — не лише тому, що вони отримують кращий захист, але й тому, що це також полегшує їм налаштування та розгортання.

Для тих захисників SOC, які часто опиняються в облозі, інтеграція на рівні продуктів SESC полегшує виконання своєї роботи. Наведемо приклад:

1. Аналітик SOC отримує інцидент від EDR, включені можливості у SESC.

2. Провівши деякі дослідження, вони визначають, як опинилася загроза у своєму оточенні.

3. Перебуваючи ще в одній консолі, вони можуть прийняти відповідну дія.

4. Крім того, вони можуть ідентифікувати та заблокувати певну модель поведінки від повторного виникнення. Ця дія досягається шляхом встановлення політики ізоляції поведінки, щоб зменшити поверхню атаки для потенційних майбутніх спроб атаки. Додатковою перевагою є те, що система мінімізує кількість сповіщень, які SOC повинні розслідувати. Тепер SOC можуть зосередитися на більш нагальних загрозах.

2. Міжпродуктова інтеграція

Symantec Integrated Cyber Defense забезпечує підвищені результати безпеки за рахунок інтеграції технологій в окремі продукти Symantec. Інтеграція інформації з кількох рішень, як локальних, так і хмарних, просто забезпечує кращу видимість загроз. Це надає більше можливостей для кореляції та застосування розвідки загроз для виявлення загроз, які в іншому випадку могли б бути пропущені, якби продукти не були інтегровані. Це також скорочує час відповіді між моментом виявлення підозрілого файлу та моментом його блокування.

Наприклад, Symantec Integrated Cyber Defense об'єднує агентів між Symantec Web Security Service (WSS) і SEP. Консолідація агентів має вирішальне значення для підтримки нижчих операційних витрат, кращого стану безпеки та кращого захисту. Єдиний агент для SEP, EDR і WSS забезпечує легке розгортання між продуктами, менше часу на керування

агентами та підвищений захист, оскільки продуктам легше працювати разом для виявлення та блокування загроз.

Інтеграція між продуктами відіграє життєво важливу роль у зусиллях із цифрової трансформації. У міру того, як все більше компаній переходять від локальних рішень до хмарних сервісів і сервісів на основі SaaS, вони стикаються з новими викликами та вимогами під час налаштування свого середовища. Більше, ніж будь-коли, їм знадобляться рішення, які допоможуть їм успішно спроектувати цю трансформацію безпечним способом. Їм потрібна здатність розуміти, хто, які типи даних отримує доступ і звідки. WSS і Symantec CloudSOC (CASB) поширюють політику відповідності даних на віддалені офіси та віддалених користувачів, не впливаючи на трафік до центру обробки даних. Інтегровані продукти перевіряють трафік під час завантаження та завантаження та застосовують політики на відповідність вимогам. Поєднуючи інтеграцію WSS (фільтрація URL + AV) + CloudSOC, політики CloudSOC перевіряються на WSS і в разі порушення наказують WSS заблокувати трафік.

Процкс використання Symantec Information Centric Analytics (ICA) для виявлення внутрішніх загроз. ICA – це платформа для аналізу поведінки користувачів і організацій, яка при інтеграції з Symantec Data Loss Prevention (DLP), SEP і CASB дозволяє швидко виявляти внутрішні загрози і кіберпорушення. Завдяки централізованій аналітиці, широким інформаційним панелям і поглибленим показникам ICA загострює ті проблеми, які в іншому випадку могли б залишитися непоміченими або вимагати складного аналізу. Завдяки автоматизованим рекомендаціям щодо виправлення ситуації ICA надає організаціям видимість і робочі процеси, необхідні для безпосереднього зменшення впливу складних загроз, значно скорочуючи ручні зусилля. Наприклад, ICA інтегрує оцінку порушень правил у DLP, кінцевих точках і хмарних системах, а також застосовує аналітику користувачів, щоб створити

повний контекст навколо схеми викрадення даних, яку здійснює незадоволений працівник. В іншому прикладі, якщо є докази скомпрометації системи або облікового запису в результаті зараження шкідливим програмним забезпеченням у поєднанні з інцидентом політики DLP з високим ризиком, ICA синтезує ці фактори для візуалізації та пом'якшення наслідків зовнішньої атаки.

3. Інтеграція зі сторонніми рішеннями

Щоб розширити можливості організацій для оптимізації стека безпеки, Symantec Integrated Cyber Defense дозволяє інтегрувати сторонні рішення через Integrated Cyber Defense Exchange (ICDx), обмін даними технологія обміну подіями та розвідувальною інформацією між системами Symantec та сторонніми системами. До ICDx користувачі, які потребували захисту в різних контрольних точках, повинні були розробити власне рішення для збору телеметрії в контрольних точках і нормалізувати її, щоб вони могли співвіднести цю телеметрію. За допомогою ICDx користувачі, по суті, отримують нормалізацію даних plug and play, централізуючи телеметрію загроз для кращого пошуку загроз.

Відкрита архітектура Symantec Integrated Cyber Defense дозволяє легко інтегрувати продукти сторонніх виробників і обмінюватися розвідувальними даними. Багатий набір відкритих API значно спрощує інтеграцію з Symantec Integrated Cyber Defense. Ця інтеграція забезпечує покращений захист, дослідження та виправлення в кінцевих точках, мережах, електронній пошті та хмарних програмах організації. Понад 120 сертифікованих технологічних партнерів, які надають 250+ додатків і послуг, створюють найширшу екосистему кібербезпеки, забезпечуючи скоординований і найкращий у своєму класі підхід до захисту, виявлення та реагування на загрози. Клієнти самі вибирають, що найкраще підходить для їхнього середовища. Яким би не було їхнє рішення, інтеграція Symantec Integrated Cyber Defense сприятиме досягненню спільної мети – створенню більш надійної екосистеми безпеки та

допоможе клієнтам притупити спроби супротивників. У підсумку клієнти можуть використовувати продукти безпеки, які доповнюють один одного, і отримують більш ефективну безпеку за зниженою ціною.

Одним із прикладів інтеграції в стек безпеки є поєднання ICDx + EDR для загроз, що розвиваються, і розширеної діяльності з виявлення та реагування. Інтеграція дозволяє ICDx збирати телеметрію загроз з усіх кінцевих точок, нормалізувати ці дані, а потім ділитися ними. Комбінація security.cloud електронної пошти ICDx + для загроз, що розвиваються, додатково підтримує розширене виявлення та реагування. Ця інтеграція надає аналітику щодо електронної пошти, кінцевих точок, Інтернету, мережі, запобігання втраті даних тощо. Розвідувальні дані можуть бути інтегровані у ваше середовище безпеки для швидшої та ефективнішої кореляції та реагування.

1.2.2 Fortinet Security Fabric

Fortinet Security Fabric розроблена компанією Fortinet, яка є одним із світових лідерів у сфері кібербезпеки. Fortinet є міжнародним постачальником інтегрованих рішень для захисту мереж інформаційних систем, ендпоінтів, облачних середовищ і даних. Штаб-квартира компанії знаходиться в США.[12]

Fortinet Security Fabric вирішує різні проблеми безпеки, забезпечуючи широку видимість і контроль всієї поверхні цифрової атаки організації для мінімізації ризику, інтегроване рішення, яке знижує складність підтримки багатоточкових продуктів, і автоматизований робочий процес для збільшення швидкості роботи.

Fortinet Security Fabric дозволяє декільком технологіям безпеки безперебійно працювати разом, у всіх середовищах і підтримуватися одним джерелом інформації про загрози під однією консоллю. Це усуває прогалини в безпеці мережі та прискорює реагування на атаки та порушення.

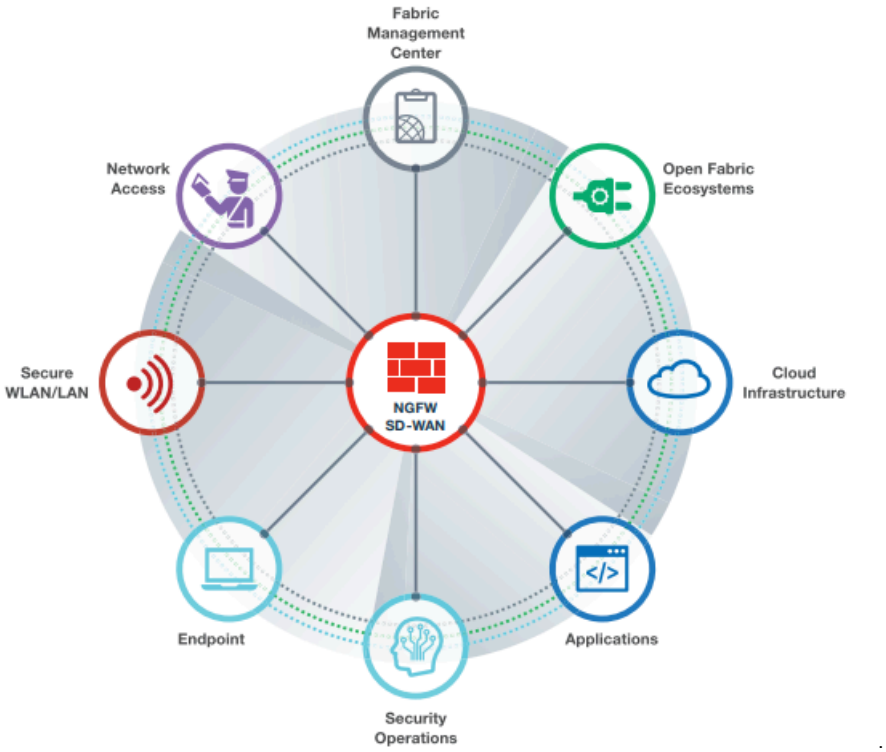

Рисунок 1.3 — Технології безпеки в Fortinet Security Fabric

У міру того, як організаційні периметри розширюються в результаті трансформацій цифових інновацій, розширюється і поверхня атаки. Fortinet Security Fabric вирішує проблему розширення поверхні атаки, надаючи організації наскрізну безпеку та видимість у всій мережевій інфраструктурі. Завдяки найширшому спектру високопродуктивних мережевих рішень, орієнтованих на безпеку, для центрів обробки даних, філій і малого бізнесу, а також для всіх основних постачальників хмарних послуг, Fortinet Security Fabric гнучко підходить для захисту кожного сегмента мережі.

Всі компоненти налаштовуються, управляються і контролюються з єдиної централізованої системи управління. На додаток до усунення розрізненості, пов'язаної з інфраструктурами безпеки точкових продуктів, єдиний інтерфейс для всіх компонентів безпеки знижує навантаження на ощадливий персонал. Система управління також сприяє розгортанню дистанційних компонентів без

дотику, заощаджуючи рулони вантажівок і ще більше знижуючи експлуатаційні витрати.

Завдяки всім компонентам, керованим однією операційною системою мережі FortiOS, Fortinet Security Fabric забезпечує узгоджену конфігурацію та управління політиками, а також легкий зв'язок у режимі реального часу через інфраструктуру безпеки. Це мінімізує час виявлення та пом'якшення загроз, знижує ризики безпеки, пов'язані з помилками конфігурації та ручним збором даних, а також сприяє своєчасному та точному реагуванню на аудит відповідності.

На додаток до інтеграції продуктів і рішень Fortinet, Security Fabric включає в себе готові з'єднання інтерфейсу прикладного програмування (API) для більш ніж 70 партнерів Fabric-Ready, які забезпечують глибоку інтеграцію між усіма елементами Security Fabric.

Для продуктів безпеки, які не є частиною екосистеми Fabric-Ready Partner, API передачі репрезентативного стану (REST) і сценарії операцій розробки (DevOps) дозволяють клієнтам легко і швидко додавати їх до Security Fabric.

На додаток до безшовної інтеграції, Fortinet Security Fabric є лідером у галузі застосування технологій машинного навчання (ML), щоб йти в ногу з ландшафтом кіберзагроз, що швидко розвивається. Fortinet Security Fabric включає розширені можливості оркестрування, автоматизації та реагування (SOAR), а також проактивне виявлення загроз, кореляцію загроз, сповіщення про обмін розвідувальною інформацією, а також дослідження та аналіз загроз.

Прискорення заходів з реагування на інциденти також вимагає забезпечення того, щоб персонал служби безпеки не відволікався на інші проблеми, такі як збір даних і створення звітів про відповідність нормативним вимогам або вищому керівництву. Тут Fortinet Security Fabric пропонує

автоматичну агрегацію журналів, кореляцію даних і генерацію звітів за допомогою вбудованих шаблонів.

Fortinet Security Fabric надає рішення в п'яти ключових областях: доступ з нульовою довірою, мережі, засновані на безпеці, динамічна хмарна безпека, операції безпеки на основі штучного інтелекту та екосистема альянсу. Кожне з них включає найкращі у своєму класі, відзначені нагородами рішення, які були оцінені та рекомендовані провідними сторонніми тестами, такими як NSS Labs, і визнані провідними аналітиками, такими як Gartner.

Рисунок 1.4 — Концептуальна основа для Fortinet Security Fabric

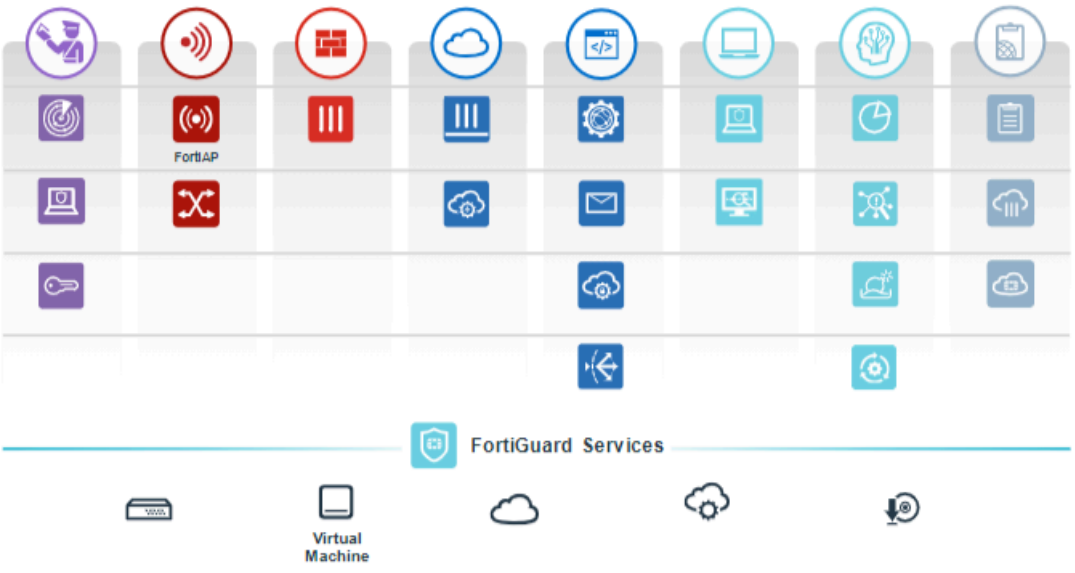

Рисунок 1.5 — Ключові пропозиції в кожній з областей рішення Security Fabric

У міру того, як кіберзагрози стають все більш складними, моделі безпеки, орієнтованої на периметр, стає недостатньо. Крадіжка облікових даних і шкідливе програмне забезпечення дозволяють зовнішнім загрозам отримати доступ до законних облікових записів у корпоративній мережі. Fortinet Security Fabric дозволяє компаніям впроваджувати політику доступу до мережі з нульовою довірою по всій корпоративній глобальній мережі.

Першим кроком у забезпеченні доступу з нульовою довірою в мережі є виявлення пристроїв, підключених до мережі. Рішення FortiNAC для контролю доступу до мережі (NAC) забезпечують автоматизоване виявлення пристроїв, що підключаються до корпоративної глобальної мережі. Підключені пристрої піддаються скануванню системи безпеки, і команда безпеки організації може визначити політики для конкретних пристроїв, які потрібно застосовувати. Після того, як пристрій схвалено для доступу до мережі, він постійно відстежується, щоб виявити будь-які поведінкові аномалії, які можуть вказувати на зараження або використання зловмисником.

Маючи можливість ідентифікувати пристрої, підключені до мережі, організації можуть реалізувати доступ із нульовою довірою, щоб визначити, хто використовує ці пристрої. Сервер управління ідентифікацією користувачів FortiAuthenticator пропонує вбудовану аутентифікацію та контроль доступу на основі ролей (RBAC), що дозволяє організаціям впроваджувати найменші привілеї та розподіл обов'язків у своїх мережах. Токени двофакторної автентифікації FortiToken посилюють аутентифікацію користувачів, дозволяючи багатофакторну автентифікацію. Це гарантує, що скомпрометовані облікові дані користувача не нададуть зловмиснику автентифікований доступ до облікового запису користувача.

Коли пристрої підключені до корпоративної мережі, через мережу можна здійснювати моніторинг пристроїв і застосування політик. Однак корпоративне використання мобільних пристроїв швидко зростає, тому корпоративні пристрої можна використовувати в автономному режимі або в інших мережах. Установка FortiClient Fabric Agent забезпечує видимість кінцевих точок і реалізує динамічний контроль доступу як в корпоративній мережі, так і поза нею.

У міру того, як корпоративні мережі та поверхні атак розширюються за допомогою DI, потреба в захисті цих мереж зростає. Мережі, керовані безпекою, тісно інтегрують мережеву інфраструктуру організації та архітектуру безпеки, дозволяючи мережі масштабуватися та змінюватися без шкоди для безпеки. Така інтеграція знижує трудомісткість за рахунок мінімізації кількості різнорідних точкових добутків. Це також дозволяє легко використовувати покращення продуктивності, оскільки мережеві пристрої та пристрої безпеки оптимізовані для спільної роботи.

Мережі, керовані безпекою, виходять на перший план у брандмауерах нового покоління FortiGate; Вони є першою лінією оборони організації від передових загроз. Однак це набагато більше, ніж брандмауери. Оскільки майже третина витоків даних пов'язана з фішинговими атаками, які покладаються на шкідливі посилання або вкладення для зараження кінцевих точок або крадіжки облікових даних користувачів, FortiGate NGFW включають безпечний веб-шлюз , який виявляє та блокує спроби підключення до шкідливих або підозрілих URL-адрес.

FortiGate NGFW також виконують розшифровку та перевірку пакетів безпеки на рівні захищених сокетів (SSL)/транспортного рівня (TLS). Сьогодні це критично важлива вимога, оскільки, за оцінками, 75% трафіку корпоративної мережі захищено за допомогою SSL/TLS, а близько 82% шкідливого трафіку використовується шифрування. В FortiGate NGFW

використовують спеціально створені процесори безпеки (SPU) для мінімізації впливу на продуктивність перевірки трафіку SSL/TLS. Інтеграція високопродуктивної перевірки зашифрованого трафіку в NGFW організації також дозволяє бізнесу уникнути накладних витрат, пов'язаних з придбанням і розгортанням автономних пристроїв у всій мережевій інфраструктурі.

Якщо загрози залишаються непоміченими по периметру мережі, важливо запобігти їх бічному переміщенню по всій мережі. Сегментація на основі намірів дозволяє організаціям безболісно досягти цього за допомогою забезпечення можливості сегментації мережі відповідно до потреб бізнесу. Підозрілі або шкідливі внутрішні з'єднання блокуються за замовчуванням, і якщо після зараження виявлено загрозу нульового дня, інформація про загрози передається через Security Fabric, щоб гарантувати відсутність вторинного зараження.

Щоб це працювало, організації потрібна інтеграція безпеки у всій корпоративній мережі, включно з філіями. Fortinet Secure SD-WAN забезпечує оптимізовану продуктивність мережі та інтеграцію безпеки для філій. FortiGate NGFW, інтегровані в пристрої SD-WAN, виконують інспекцію дорожнього руху в кожному відділенні. Це підвищує продуктивність мережі, забезпечуючи пряме підключення до Інтернету для SaaS-додатків і послуг, а також дозволяє знизити витрати на WAN.

У межах філії Fortinet Secure SD-Branch дозволяє розширити видимість організації та централізоване управління безпекою аж до рівня комутації. Fortinet Secure SD-Branch складається з рішень FortiNAC, захищених комутаторів доступу FortiSwitch і бездротових точок доступу FortiAP, які контролюються і управляються з FortiGate NGFW. Інтегруючи безпеку в корпоративні глобальні мережі, компанії спрощують операції, усуваючи надмірність, і забезпечують швидке, скоординоване реагування на складні загрози.

Оскільки організації переходять на хмару, розширення розгортання безпеки організації на хмарні ресурси має важливе значення. Fortinet Security Fabric інтегрує ряд хмарних рішень для забезпечення безпеки будь-яких додатків і середовищ розгортання.

Рішення безпеки Fortinet пропонують мережеву безпеку, видимість і контроль як в публічних, так і в приватних хмарних розгортаннях. FortiGate NGFW доступні у форм-факторі віртуальних машин. Це дозволяє їм забезпечувати хмарну автоматизацію безпеки, підключення до VPN, сегментацію мережі, запобігання вторгнень і SWG.

Окрім захисту від шкідливого вмісту, організації також повинні забезпечити належне налаштування своїх хмарних розгортань. Неправильні конфігурації безпеки є основною проблемою в загальнодоступній хмарі, при цьому 99% проблем залишаються незареєстрованими. Аналітика хмарної безпеки FortiCWP забезпечує видимість і контроль в публічній хмарній інфраструктурі, включаючи моніторинг конфігурацій, безпеки даних і відповідності, а також інтегроване управління загрозами.

Після того, як сама хмарна інфраструктура захищена, необхідно захистити запущені на ній додатки. Поширеним використанням розгортань загальнодоступних хмар є розміщення веб-додатків і веб-API. FortiWeb забезпечує їм хмарну безпеку. Брандмауери веб-додатків FortiWeb (WAF) захищають веб-додатки як від відомих, так і від невідомих загроз за допомогою комбінації виявлення сигнатур, машинного навчання та штучного інтелекту. Крім того, оскільки більшість веб-додатків використовують API для зв'язку з веб-службами та інтеграції з іншими інструментами, дуже важливо захистити ці веб-API за допомогою перевірки схеми та безпеки OpenAPI для захисту від потенційно шкідливих дій ботів, таких як скрейпінг та аналітика.

Організації також все частіше переходять на хмарні рішення для електронної пошти, такі як Google G Suite і Microsoft Office 365. Оскільки

фішингові атаки є основною причиною інцидентів безпеки та витоку даних, захист хмарної електронної пошти має важливе значення. Доступні як фізичні та віртуальні пристрої або як розміщена служба, рішення безпеки обміну повідомленнями FortiMail захищають як локальні, так і хмарні розгортання електронної пошти, включаючи блокування традиційних і розширених загроз електронної пошти та надання функцій резервного копіювання, щоб уникнути втрати конфіденційної інформації.

Окрім веб-додатків та електронної пошти, багато організацій покладаються на SaaS-програми, такі як Google G Suite, Box, Microsoft Office 365, Dropbox і Salesforce. Брокери безпеки хмарного доступу (CASB) FortiCASB управляють ризиками неправильної конфігурації безпеки, забезпечують централізовану видимість і адміністративний контроль, забезпечують безпеку даних в SaaS-додатках і гарантують, що конфігурації додатків SaaS відповідають нормативним вимогам.

Збільшений обсяг і складність зловмисних атак роблять традиційні рішення з кібербезпеки недостатніми. Рішення для виявлення шкідливих програм на основі сигнатур здатні виявити лише половину атак шкідливого програмного забезпечення. Використання можливостей штучного інтелекту та машинного навчання має важливе значення для виявлення та запобігання цим атакам.

FortiGuard AI дозволяє організаціям випереджати кіберзлочинців. FortiGuard Labs збирає дані про загрози з мільйонів датчиків по всьому світу та співпрацює з більш ніж 200 глобальними організаціями. Використовуючи понад 5 мільярдів вузлів, FortiGuard AI визначає унікальні функції як для відомих, так і для невідомих загроз. Обсяги, які обробляє FortiGuard Labs, величезні: команда обробляє понад 100 мільярдів веб-запитів щодня і блокує понад 3600 шкідливих URL-запитів щосекунди.

У міру того, як загрози стають дедалі складнішими, 100% запобігання стає неможливим. Розширені можливості виявлення загроз мають важливе значення для того, щоб допомогти організаціям уникнути порушень. Можливості штучного інтелекту та машинного навчання, інтегровані в FortiDeceptor, FortiSandbox та FortiInsight, допомагають організаціям виявляти невідомих зловмисників та шкідливе програмне забезпечення, а також виявляти внутрішні загрози та реагувати на них.

У міру того, як кіберзагрози прискорюються, організації повинні скористатися перевагами стратегічної автоматизації для більш швидкого стримування та усунення загроз. Використовуючи FortiSIEM і FortiAnalyzer, організація може досягти глобальної видимості своєї мережевої інфраструктури і отримати доступ до аналітики безпеки на основі штучного інтелекту. На основі зібраних даних аналітики безпеки можуть визначити характер і серйозність загроз за підтримки віртуального аналітика FortiAI. Але він не зупиняється на виявленні та запобіганні загрозам; FortiSOAR використовує оркестрацію та автоматизацію для усунення вторгнень загроз, які допомагають перевантаженим командам операційних центрів безпеки (SOC) масштабуватися та зосередитися на пошуку загроз та інших критично важливих завданнях.

Кінцеві точки також потребують ресурсів на основі штучного інтелекту протягом усього процесу реагування на інциденти. FortiEDR endpoint detection and response (EDR) і FortiClient забезпечують розширений захист кінцевих точок, який включає сканування вразливостей, виправлення, а також віртуальне виправлення та запобігання експлойтам як в онлайн-середовищах, так і в середовищах з повітряним зазором. Крім того, якщо кінцева точка заражається, виявлення загроз FortiEDR і захист після зараження запобігає зв'язку шкідливого програмного забезпечення з командно-контрольними серверами або бічному переміщенню по мережі. Нарешті, FortiEDR пропонує реагування

на загрози на основі оцінки ризиків та онлайн-виправлення з підтримкою автоматизованих рецептів виправлення.

Fortinet Security Fabric призначена для спрощення управління всією архітектурою безпеки організації. Fabric досягає цього шляхом інтеграції всіх розгорнутих точок безпеки, що дозволяє централізовано контролювати та керувати ними.

Платформа централізованого управління FortiManager і централізована реєстрація та звітність FortiAnalyzer об'єднуються, щоб забезпечити видимість і управління всією мережевою інфраструктурою організації. Це включає в себе управління єдиною консоллю, аналітику та автоматизацію робочих процесів.

Ці можливості підтримуються рядом інтеграцій на основі API з партнерами Fortinet Fabric-Ready. Дванадцять з'єднувачів Fabric забезпечують глибоку інтеграцію зі сторонніми рішеннями, а інтеграція на основі API доступна для більш ніж 135 партнерів, готових до роботи з тканиною. Для рішень, які не є партнерами, Fortinet Security Fabric включає REST API та сценарії DevOps для легкої інтеграції.

Оскільки багато організацій переносять операції в хмару, для зменшення складності мультихмарного розгортання необхідне рішення з єдиною точкою доступу та єдиним входом (SSO). FortiCloud надає SSO та портали до 15 рішень Fortinet SaaS та Metal-as-a-Service (MaaS), а також портал послуг FortiCare. Завдяки підтримці всіх основних постачальників публічних хмар, Fortinet Security Fabric спрощує будь-яке мультихмарне розгортання.

Об'єднавши FortiManager, FortiAnalyzer і FortiCloud, організація може повністю інтегрувати свої локальні та хмарні розгортання. Ця інтеграція дозволяє використовувати автоматизацію та оркестрацію для спрощення керування безпекою. Крім того, використовуючи Fabric Connectors і API, команди безпеки можуть отримувати інформацію про стан мережі в режимі

реального часу, автоматизувати керування мережевими журналами та спростити звітування про відповідність вимогам, і все це з однієї панелі.

Цифрові інновації дозволяють організаціям досягати нових рівнів ефективності та економії коштів для себе, а також покращувати досвід для своїх клієнтів. Однак ініціативи цифрових інновацій також розширюють і змінюють поверхню атаки організації, відкриваючи нові вектори атак для використання кіберзагроз.

Для організацій, які лідирують у сфері цифрових інновацій, визнання, прийняття та належне управління ризиками має першорядне значення. Основою для цього є захисна тканина Fortinet. Він об'єднує рішення безпеки за єдиною панеллю, робить видимою зростаючу поверхню цифрової атаки, інтегрує запобігання зламам на основі штучного інтелекту та автоматизує операції, оркестрування та відповідь. У підсумку, це дозволяє організаціям створювати нову цінність за допомогою цифрових інновацій без шкоди для безпеки для гнучкості, продуктивності та простоти бізнесу.

РОЗДІЛ 2 ЕТАПИ СТВОРЕННЯ КСЗІ НА ПІДПРИЄМСТВІ ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС»

2.1 Недоліки СЗІ на підприємстві ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС»

Особливістю ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС» (далі – «Автолюкс») є високий рівень сервісу та комфорту пасажирів.

Вони забезпечують комфортні сидіння, кондиціонери, біохімічні туалети та мультимедійні розважальні засоби у своїх автобусах. Це дозволяє пасажирам комфортно подорожувати та насолоджуватися поїздкою. Без цієї компанії важко уявити транспортну інфраструктуру, яка б не покращилась у плані зручностей та послуг. Компанія «Автолюкс» встановила високі стандарти якості обслуговування, завдяки чому займає лідируючі позиції на ринку пасажирських перевезень. Їхні послуги особливо популярні на далеких маршрутах, де комфорт і зручність відіграють важливу роль при виборі перевізника. Ця компанія охоплює велику кількість різноманітних послуг, але нас цікавить лише одна з них – інформаційно-комунікаційні послуги.

Основною функцією служби є забезпечення надійної роботи засобів зв’язку, радіозв’язку, хронометражу, автоматизованих систем управління технологічними процесами, автоматизованих систем оплати проїзду та апаратно-програмних комплексів автоматизованих виробничих процесів, мережевої інфраструктури, комп’ютерів, серверів, технічне обслуговування та розвиток. корпоративного офісного обладнання та програмного забезпечення інформаційних систем.

З метою забезпечення комфортного життя та безпечних подорожей людей, дане підприємство повинно мати найсучасніше програмне та технічне забезпечення. Крім того, необхідно мати систему захисту інформації, яка запобігає використанню різноманітних методів доступу до конфіденційних даних та ресурсів, включаючи фізичний та програмний доступ. ТОВ "ААЗ

ТРЕЙДІНГ-АВТОЛЮКС" складається з багатьох взаємопов'язаних служб та відділів, які також повинні бути належним чином захищені. Якщо захист одного відділу буде недостатнім, це може негативно вплинути на роботу інших відділів та загрожувати функціонуванню всього підприємства. Найгіршим наслідком порушення роботи підприємства є можлива втрата життя пасажирів, тому необхідно прикласти максимум зусиль до захисту інформації.

У мене була інформація про роботу інженерно-технічного відділу, тому в кваліфікаційній роботі я врахував СЗІ цього предмету. Я зосереджений на технологічній та програмній частині бізнесу. У таблиці 1.1 наведено контрольний список технічної підтримки на робочому місці.

Таблиця 1.1 - Технічне забезпечення робочих місць

№	Назва	Модель	Номер	Виробник
1	Системний блок Монітор Клавіатура Комп’ютерна миша	Vostro 3471 P2419H X500 KB216	101480077 G879969K KI578KJ JHB7890L	Dell Dell HP Dell
2	Системний блок Монітор Клавіатура Комп’ютерна миша	Vostro 3471 P2419H X500 KB216	DCTJV465 578599KVGH 67858KJL YDVFJ898	Dell Dell HP Dell
3	Сервер	PowerEdge T40	FKJAS7688	Dell
4	Мережевий екран	ASA 5506-X	7648H19827	Cisco Systems

Одною з проблем SHI була недостатня безпека на її серверах, включаючи сервери резервного копіювання та сервери, які обробляють і зберігають робочу інформацію. Проблема полягає в некоректному розмежуванні прав доступу до технічного обладнання. Кожен системний адміністратор має достатній доступ до сервера. Якщо зловмисник отримує доступ до будь-якого комп’ютера адміністратора, він може отримати доступ до сервера з обмеженням доступу.

Іншою проблемою цього програмного забезпечення є брандмауер, налаштований на екрані мережі. Виявилося, що мережевий щит мав відкриті

порти які не використовуються. Щодня з’являються нові способи проникнення в системи, а ймовірність того, що зловмисник отримає доступ до системи збільшується через ці відкриті порти, отже, він отримає доступ до інформації компанії.

На території суб’єкта є бездротова мережа Wi-Fi, тому необхідно враховувати пов'язані з цією мережею загрози. В середовищі, де сигнали передаються через бездротові мережі, отримати інформацію набагато легше, ніж у дротовій мережі. Для цього просто розмістіть антену в радіусі роботи бездротової мережі. Точки доступу також можна клонувати. Злодію необхідно тільки надати достатньої потужності сигнал і визначити SSID точки, де він хоче клонувати.

Необхідно також пам'ятати про DoS-атаки, які часто виконуються на основі WPA. Зловмисник відправляє 2 пакета з випадковими ключами шифрування кожну секунду, що призводить до того, що точка доступу, яка отримує дані пакети, визначає, що попитка отримання несанкціонованого доступу була здійснена і закриває всі з'єднання.

Політика BYOD – Принесіть свій власний пристрій стає ще однією загрозою для бізнесу. На превеликий жаль, мало хто знає достатньо про безпеку в Інтернеті та можуть ненавмисно встановити шкідливе ПЗ на своїх пристроїх. Коли особистий пристрій підключено до корпоративної мережі, зловмисне програмне забезпечення може проникнути в мережу та встановити себе на комп’ютерах або серверах співробітників, які містять важливу інформацію.

У закладі між кабінетами встановлено пластикові міжкімнатні перегородки, які не забезпечували належного захисту від витоку аудіоінформації. Коли в офісі обговорюється важлива інформація, її можна прослухати навіть без використання спеціальних засобів збору аудіоінформації та технічних засобів.

2.2 Обстеження середовищ функціонування ІТС

При здійсненні цих задач ІТС буде розглядатися організаційно-технічною системою, яка об’єднує комп’ютерну систему, середовище користувача, фізичне середовище, інформацію, що обробляється, і технології її обробки.

Мета дослідження полягає в тому, щоб описати форму кожного ІТ-середовища, підготувати базові дані для сформування правил КСЗІ, визначити елементи, які впливають на безпеку інформації, визначити взаємодію між різними елементами середовища та записати результати дослідження для подальшого використання в практика.[13]

Не варто забувати, те що операційні системи складаються з наборів, що перекриваються, різні елементи яких можуть належати до різних середовищ одночасно та мати різноманітні характеристики. Наприклад, ПЗ можна розглядати як активний процес у комп’ютерній системі, в той час в інформаційній системі воно може розглядаться як інертний об’єкт комп’ютерної системи.

Дослідження проведено після формулювання концепції ІТС, визначення головних завдань і особливостей ІТС, функціональної сукупності ІТС та наявності варіантів її впровадження.

У процесі перевірки КС треба аналізувати та описувати такі аспекти ІТ:

- Загальне структурне планування та склад системи, включаючи перелік і склад обладнання, технології та програмного забезпечення, їх зв’язки, характеристики конфігурації, архітектуру та топологію, програмне та апаратне забезпечення, апаратне забезпечення та інформаційну безпеку, взаємне розміщення інструментів і так далі ;
- Види та особливості каналів зв'язку;
- Характеристика кожного компонента та їх взаємодія;
- Допустимі обмеження до користування засобами.

Необхідно визначити, які компоненти комп’ютерної системи мають, а які не мають засоби та механізми захисту інформації, потенційні можливості цих засобів та механізмів, їх властивості та характеристики, у тому числі встановлені за замовчуванням. Мета цього аналізу полягає в тому, щоб отримати уявлення про наявність потенційних можливостей для забезпечення захисту інформації, визначити компоненти ІТС, які вимагають додаткових вимог до захисту, і запровадити додаткові заходи безпеки.

У процесі перевірки інформаційного середовища важливо ретельно проаналізувати всі дані та програмне забезпечення, що зберігаються та обробляються в ІТС. Цей аналіз включає класифікацію інформації на основі методу доступу та правової системи, а також визначення та опис способу, яким вона подається до ITS з точки зору CS. Кожен тип інформації та об’єктів, які вона охоплює, мають специфічні атрибути, пов’язані з інформаційною безпекою (конфіденційність, цілісність, доступність) або CS (спостережливість). Крім того, аналіз технологій обробки інформації має на меті виявити характеристики електронних документів, окреслити інформаційний потік і середовище його передачі, визначити джерело та місце призначення інформаційного потоку, встановити принципи та методи управління потоком і створити діаграму потоку. . Додатково документується тип носія інформації та послідовність його використання в процесі функціонування ІТС. Схема інформаційного потоку аналізується з точки зору її структурних елементів, включаючи склад інформаційного об’єкта, режим доступу, потенційний вплив середовища користувача та роль фізичного середовища у збереженні властивостей інформації.

Вивчення фізичного середовища передбачає вивчення розміщення засобів обробки ІТ-інформації в сфері інформаційної діяльності, зв’язку та систем життєзабезпечення. Додатково аналізуються режими роботи цих об'єктів. Під час перевірки обов’язково дотримуватись вимог ДСТУ 3396.1.[1]

Для повного розуміння інформаційно-телекомунікаційної системи (ІТС) вкрай важливо вивчити різні аспекти її фізичного середовища, такі як

- розміщення елементів ІТС, охоплюючи загальне планування, сценарне планування, захист території і систем обходів;

- категорійовані приміщення для розташування компонентів ІТС;

- порядок доступу до фізичних елементів середовища ІТС;

- фактор довкілля, задля уникнення впливів технічних розвідок;

- наявність засобів та способів зв'язку, системи забезпечення та компонентів зв'язку за територією підконтрольних зон;

- наявність системи заземлення та її ТХ;

- правила та рекомендації зі зберігання інформаційних носіїв, а саме - паперові носії, магнітні носії та оптично-магнітні носії;

- повинна бути документована інформація про проектування і користування фізичними компонентами середовища.

При аналізі середовища користувача проводиться оцінка:

- функціоналу і чисельного складу користувачів, їх функціональних обов'язків та рівня кваліфікації;

- уповноважень користувачів на отримання доступу до інформації, яка оброблюється всередині ІТС, отримання доступу до ІТС і елементів;

- повноважень до керування комплексною системою захисту інформації (КСЗІ);

- гарантування можливостей для всіх типів користувачів, котрі можуть надаватися за допомогою засобів ІТС;

- наявнсть систем які забезпечують захист даних в ІТС.

Висновки обстеження виробничого середовища в ІТС оформляються у вигляді офіційного звіту. За потреби ці висновки вносяться до відповідного розділу плану захисту інформації ІТС, який відповідає рекомендаціям,

викладеним у НД ТЗІ 1.4-001.[2] За результатом оцінки робочого середовища ІТ затверджено перелік захищених активів з врахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо об’єкта класифікації. [2; 3; 4] Крім того, ідентифікуються потенційні інформаційні загрози та розробляються як модель загрози, так і модель порушника. Створення цих моделей відповідає стандартам НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 і НД ТЗІ 1.6-002.[5; 2; 6] Пропонується, щоб модель інформаційної загрози та модель порушника були представлені як окремі документи або, альтернативно, об’єднані в один документ у рамках плану захисту.

На початковому етапі розробки КСЗІ було встановлено наступні аспекти: мета захисту інформації у сфері ІТ, мета створення КСЗІ та підхід до вирішення проблеми безпеки на основі ДСТУ 3396.1 [1].

Було проведено комплексну оцінку ризику, яка передбачала дослідження як моделі загрози, так і моделі правопорушника. Аналіз також враховував потенційні результати впровадження цих загроз, а також розмір потенційних втрат.

Визначення загальної структури та складу КСЗІ, а також вимог до заходів інформаційної захищеності, допустимих обмежень, обмежень на використання ресурсів, умов створення та функціонування КСЗІ, а також загальних вимог до різних підсистем і компонентів, у тому числі застосування заходів захисту, все це невід’ємні аспекти, які сприяють формуванню КСЗІ.

Формується звіт щодо здійснення цього етапу і розроблення програм КСЗІ, таких як тактико-технічні завдання або інші аналогічні документи.[5]

2.3 Розробка політики безпеки інформації в ІТС

На початковому етапі розробки КСЗІ розробники ретельно вивчають об’єкт, на якому буде створюватися КСЗІ. Це обстеження передбачає комплексний аналіз об’єкта, включаючи виявлення потенційних загроз, порушень та оцінку можливостей об’єкта щодо управління ризиками. Крім того,

розробники проводять масштабні дослідження для вивчення різних підходів до реалізації завдання створення КСЗІ. Також працюють над розробкою плану проекту та підготовкою звітів для НДР.

2.3.1 Оформлення політики безпеки

На даний момент визначено основні стратегії для усунення значних ризиків, а також розроблено керівні принципи, правила, обмеження, рекомендації та інші заходи для керування використанням безпечних технологій обробки інформації в сфері ІТ. Крім того, було викладено особисті заходи безпеки та захисні заходи, а також обов’язки всіх користувачів.

Зараз триває розробка документів політики інформаційної безпеки. Політика безпеки може бути створена для всієї системи інформаційних технологій (ІТС), або, якщо окремі компоненти КСЗІ вимагають особливої уваги, політики безпеки можуть бути сформульовані для кожного окремого компонента, функціонального завдання або технології обробки інформації. Формулювання політики безпеки відповідає керівним принципам, викладеним у нормах НД ТЗІ 1.1-002, і рекомендаціям, наданим у документі НД ТЗІ 1.4-001. [5, 2] Доцільно створити окремий документ, відомий як План захисту, щоб окреслити стратегію безпеки.

Рішення, що стосуються наступного етапу роботи, включаючи проектні рішення, організацію роботи, розподіл відповідальності, процедури впровадження та функціонування КСЗІ, безпосередньо пов’язані з положеннями, викладеними в політиці безпеки. Ці рішення документуються та приймаються на відповідній стадії, за винятком фактичного виконання робіт. Хоча в технічному завданні на створення КСЗІ можуть бути визначені вимоги до виконання робіт, воно все ж має відповідати етапам, зазначеним у ТУ.

2.4 Розробка технічного завдання на створення КСЗІ

Основний документ, який визначає вимоги до захисту інформації в ITS, а також процес розробки КСЗІ, проведення тестів і впровадження КСЗІ, відомий як технічне завдання на створення КСЗІ в ІТС. На початкових етапах розробки ІТС було сформульовано технічне завдання на створення КСЗІ з урахуванням складного підходу до побудови КСЗІ. Цей комплексний документ охоплює всі необхідні заходи та ресурси, необхідні для пом'якшення різноманітних загроз інформаційній безпеці протягом життєвого циклу ІТС. Технічне завдання на створення КСЗІ може бути розроблено, незалежно від того, чи це новостворена ІТС, чи вже існуюча, яка перебуває на модернізації.[14]

У КСЗІ є кілька варіантів реєстрації для ТЗ. Ці варіанти включають включення ТЗ як окремого компонента ТЗ для розробки ІТС, створення окремого (часткового) ТЗ або додавання ТЗ як розширення до ТЗ для створення ІТС. Важливо відзначити, що вибір варіантів реєстрації не обмежений. Перший варіант зазвичай рекомендується для початкових проектів розробки ІТС. Однак для ініціатив з модернізації КСЗІ, а також модернізації існуючих ІТС або тих, що вже мають затверджені ТЗ для створення, рекомендується другий або третій варіант. Ці варіанти виключають включення окремого розділу про захист інформації.

Для досягнення інтегрованої інтелектуальної транспортної системи (ІТС), яка базується на модульності, доцільно формалізувати вимоги КСЗІ для кожного окремого компонента ІТС в окремому документі. Також можливо створити єдиний документ для кількох схожих компонентів КСЗІ, за винятком компонента ТК, який використовується для створення ІТС, який повинен мати окремий документ із зазначенням будь-яких варіацій або унікальних характеристик.

Якщо умови роботи істотно не відрізняються, такі компоненти, як ІТС КСЗІ та КСЗІ локальних мереж зі схожими функціональними завданнями

інтегрованої ІТС, можна віднести до одного типу. Технічне завдання (ТЗ) охоплює вимоги як до окремих компонентів ІТС, так і до всієї системи, включаючи необхідність безпечної взаємодії між цими компонентами.

Щоб встановити окреме ТЗ для формування КСЗІ або розширення існуючого ТЗ для створення ІТС, важливо підтримувати послідовність у системі понять, імен та ідентифікації об'єктів, що використовуються в ТЗ для розробки ITS. . Розглядаючи будь-який альтернативний підхід до розробки та оформлення ТЗ на КСЗІ, обов'язково слід враховувати методичні рекомендації, викладені в НД ТКІ 3.7-001, які диктують вимоги до змісту, затвердження та процесу затвердження.[7]

2.5 Розробка проекту КСЗІ

Створення ІТС є фундаментом проекту КСЗІ, який базується на ТЗ. У процесі розробки проекту КСЗІ проектні рішення розробляються та перевіряються, щоб відповідати вимогам ТК, забезпечувати сумісність і взаємодію між компонентами КСЗІ, а також впроваджувати заходи та методи захисту інформації. Реалізація проекту КСЗІ відбувається в три етапи: макетний проект, технічний проект і робочий проект. Але можна виключити стадію «Ескізний проект КСЗІ» та об'єднати «Технічний проект КСЗІ» та «Робочий проект КСЗІ» в одну стадію під назвою «Технологічний робочий проект КСЗІ».

Структура документа для кожного етапу проекту КСЗІ встановлюється на основі технічних умов, викладених у НД ТЗІ 2.5-004.[8] Документована інформація програмного забезпечення відповідає стандартам, встановленим ESDP, а апаратного забезпечення відповідає стандартам ESCD.

Під час розробки макетного проекту КСЗІ, спочатку вводиться попереднє проектне рішення комплексної системи захисту. Якщо потрібно, формулюються окремі компоненти цього рішення, а також розробляється, оформлюється, узгоджується та затверджується документ на КСЗІ. Проектні рішення на рівні проекту адекватно описані в цьому документі, охоплюючи як зміст, так і стиль.

Чітко окреслені наступні аспекти: загальна функція КСЗІ та специфічні функції її різних компонентів; склад комплексу захисту інформаційних технологій, призначеного для запобігання витоку даних за технічними каналами та пом'якшення можливих спецнаслідків; протидія технічним, розвідувальним, організаційним, правовим та іншим заходам захисту; склад КЗЗ; та комплексну структуру та схему взаємодії компонентів КСЗІ. Крім того, представлені попередні технічні рішення, що забезпечують успішне виконання завдань і функцій КСЗІ.

Зараз триває процес розробки проектних рішень для Інтегрованих систем захисту інформації (ІСЗІ). Ця розробка передбачає створення комплексних проектних рішень, необхідних для виконання вимог, викладених у технічному завданні на КСЗІ. Додатково визначається структура КСЗІ, яка включає організаційну структуру, апаратно-програмну складову, алгоритми роботи та умови використання засобів захисту. Архітектура КЗП встановлюється на основі функціонального профілю послуг інформаційної безпеки та механізмів реалізації. Для забезпечення узгодженості розвитку КЗЗ, архітектури, середовища розробки, тестування, середовища експлуатації та експлуатаційних документів КЗЗ реалізуються організаційно-технічні заходи відповідно до нормативних документів НД ТЗІ 2.5-004, НД ТЗІ 2.5-008 та НД ТЗІ 2.5-010.[8; 3; 4]

У КСЗІ ведуться роботи зі створення комплексної документації, яка включає реєстрацію, узгодження та затвердження необхідних документів, як зазначено в ТЗ. Ці документи повинні ефективно передавати проектні рішення на рівні технічного проекту. Додатково готується документація на закупівлю засобів захисту інформації та/або технічні вимоги до їх розробки. Так само готуються документи на придбання засобів захисту або їх комплектуючих для включення до КСЗІ. У випадках, коли бажаний продукт недоступний на ринку

для захисних заходів, встановлюються спеціальні технічні вимоги, щоб полегшити розробку відповідних альтернатив.

Для проектування в суміжних галузях, пов'язаних з створенням комп'ютерних систем захисту інформації (КСЗІ) або інших суттєвих аспектів, таких як будівництво, електротехнічні та санітарно-технічні аспекти, необхідно розробити відповідне завдання. На етапі розробки проекту КСЗІ важливо підготувати, зареєструвати та затвердити робочу та експлуатаційну документацію для КСЗІ, а також, за потреби, окремі її складові. Робочі матеріали мають містити докладні рішення щодо впровадження технічних проектів КСЗІ, забезпечення управління та взаємодії компонентів КСЗІ, а також документацію, необхідну для тестування, налагодження та перевірки цієї системи.

В даний момент проводиться процес розробки засобів захисту інформації або адаптації готового продукту для використання в системі КСЗІ. Цей процес включає в себе створення методів захисту інформації від несанкціонованого доступу та їх відповідність вимогам, визначеним у Технічному завданні з інформаційної безпеки 3.6-001.

Задля того щоб запобігти витокам даних за допомогою технічних каналів необхідно створювати документацію з ТЗ, включаючи порядок розташування ОТЗ ІТС, кабелів, мережі електричного живлення та систем заземлення. Ці задуми формуються згідно до вимогам ТР ЕОТ-95 та ТР ТЗІ – ПЕМВН-95.[9; 10] При розробці враховуються правила розташуваннь і допустимих відстаней поміж засобами і ДТЗ, розташованими в будівлях, в яких розміщені пристрої ІТС, і в сусідніх приміщеннях. Ці умови визначаються з експлуатаційної документації, що додаються до сертифікованого ОТЗ. У випадку, якщо ОТЗ, яку використовують як частину комплексної системи захисту інформацію, не має сертифікатів відповідності вимогам щодо ТЗІ, найменш дозволена відстань і

другі вимоги розташування даних засобів мають визначатися на основі результатів спеціальних досліджень.

Для того щоб створити повну робочу документацію для КЗЗ, необхідно докладно описати процедуру встановлення та ініціалізації комплексу. Крім цього, важливо налагодити механізми розрізнення доступу юзерів до даних і зовнішніх джерел ІТС, забезпечити контроль за діяльністю користувача/чів, а також організувати формування та актуалізацію бази даних захисту. До робочого проекту слід додати інформацію для введення до бази даних захисту. Експлуатаційна документація повинна увібрати опис функціонування КСЗІ та надати настанови щодо забезпечення цього порядку обслуговуючим персоналом та користувачами. Також вона має включати порядок супроводження КСЗІ протягом життєвого циклу ІТ, зокрема інструкції щодо цього.

2.6 Підготовка КСЗІ до введення в дію

Наразі проводяться підготовчі роботи з організаційної побудови і складаються необхідні документи для керування інформаційними системами ІТС. У випадку коли цу незроблено раніше, то розробляється система захисту інформації (і призначається відповідальна особа). Підготування і утвердження документації, включеної до Плану захисту, мають завешити (винятком можуть бути ті, яким необхідні результати робіт наступних етапів). розробка системи інформаційної захищеності і розробка Плану захисту проводяться відповідно до Нормативного документу ТЗІ 1.4-001.[2]

2.7 Навчання користувачів

Всі користувачі ІТС, включаючи склад техпідтримки, звичайних користувачів та користувачів, уповноважених до управління засобами комплексної системи захисту інформації, навчаються з основних положень Плану захисту. Це навчання необхідне для того, щоб вони могли дотримуватися умов інформаційної безпеки, використовувати інструменти захисту та

перевіряти свою здатність використовувати впроваджену технологію захисту інформації. Результати навчання також реєструються.

2.8 Попередні випробування

Первинна мета проведення попереднього випробування полягає в оцінці продуктивності криптографічної системи захисту інформації (КСЗІ) та визначенні її придатності для наступного використання у дослідній експлуатації. Під час цих випробувань оцінюється функціональна ефективність КСЗІ та відповідність її технічним вимогам. Проведення попередніх випробувань здійснюється відповідно до процедур і методів, які розроблені виробниками КСЗІ та схвалені замовниками інформаційно-технічних систем (ІТС). Вказані процедури, методи та протоколи випробувань формулюються й видані відповідно вимогам, що встановлені у Регламенті безпеки й оборони 50-34.698.

Остання перевірка КСЗІ готується замовником ІТС та проводиться спільно з розробником. Комісія, утворена замовниками ІТС, проводить попередні випробування, головою якої є представник замовника. Результати випробування фіксуються у "Протоколі випробування", де вказуються підсумки до упровадження крмплексної системи захисту інформації для дослідної експлуатації, а також виявлені недоліки, заходи необхідні для їхнього усунення і планові дати завершення робіт. Коли недоліки будуть усунені та відбудеться виправлення документації КСЗІ складається акт прийому для дослідної експлуатації.

2.9 Дослідна експлуатація

У процесі проведення експериментальної роботи з комплексними системами захисту інформації (КСЗІ) використовуються різні технології, такі як управління засобами захисту, обробка інформації, обіг машинних носіїв даних, , розподіл прав доступу юзерів до джерел інформаційно-технологічної системи і

автоматизоване контролювання користувача. Працівники і користувачі інформаційно-технологічної системи отримують практичні навички використання технічних та програмно-апаратних засобів захисту інформації, ознайомлюються з вимогами організаційної і розпорядчої документації до розділу ТЗ і прав доступу в інформаційних ресурсах. При необхідності вдосконалюється програмне забезпечення, проводиться додаткове налаштування та конфігурація КСЗІ, а також вносяться коригування до робочих та експлуатаційних документів.

На підставі отриманих результатів складається акт про завершення дослідної експлуатації будь-якою формою, в якому висловлюється висновок щодо можливості (неможливості) подання комплексної схеми захисту інформації на державну експертизу.

2.10 Державна експертиза КСЗІ

Державна експертиза комплексних систем засобів інформаційно-технічного захисту (КСЗІ) представляє собою окремий етап процесу атестації ІТС. Її метою є перевірка відповідності технічним вимогам та завданням із захисту інформації, а також визначення можливості включення КСЗІ до складу інформаційно-технічних систем для подальшої експлуатації. Проведення державної експертизи КСЗІ в ІТС здійснюється відповідно до встановленого Положення про державну експертизу у галузі технічного захисту інформації. У разі виявлення дефектів під час перевірки, вони усуваються до завершення процедури, з застосуванням таких же методів, що й для попередніх тестів. У випадку, коли з будь-яких причин недоліки не можуть бути усунені під час першого огляду, складається акт, в якому вказується перелік необхідних поліпшень та рекомендації з їх виконання. Після завершення робіт, передбачених у зазначеному акті, проводиться повторна експертиза.

У контексті інтегрованої ІТС можливо проводити індивідуальну оцінку кожного модуля в рамках КСЗІ. Перевірка інтегрованого КСЗІ представляэ

собою перевірку модулів які були оцінені, обмін даних бази даних безпеки, адміністративне керування та інше. Документи, в яких містяться досягнення роботи на різних етапах для ІТС КСЗІ (сертифікати відповідності, протоколи, акти) складаються із врахуванням відповідної документації на складові КСЗІ. Якщо інтегровані комплексні системи захисту містять базові модулі, які створюються щоб задовольнити потреби 1 технічного засобу, експертна оцінка цих модулів КСЗІ здійснюється протягом двох етапів: 1 – комплексна перевірка обраного типового модуля, 2 – контроль відповідності діючим умовам кожному конкретному об'єкту які існують в модулях КСЗІ.

При включенні нових доповнень в КСЗІ яка наразі існує не потрібно проводити повторну оцінку всієї системи. Триває оцінка взаємодії цього додатка з елементом КСЗІ, який зараз функціонує. Стан КСЗІ можна оцінювати одночасно з етапами проектування. Такий порядок пропонується для складних за архітектурою, композицією та масштабом робіт об’єктів, які виконує КСЗІ. Професіонали регулярно проводять оцінку технічних та організаційних рішень на кожному етапі своєї роботи. Насамперед це надає дозвіл дуже швидко виявляти та усувати недоліки, тим самим скорочуючи тривалість експертного оцінювання, яке можуть закінчити до приймального етапу іспитів для ІТС. Приймальний іспит ІТС проводиться на повністю працездатному КСЗІ. Робота виконана використовуючи тестові дані, які не включають ІЗОД.

Дотримуючись розрахунків захисту і експлуатаційної документації на складові КСЗІ проводяться роботи з посилення організаційного функціонування КСЗІ, удосконалення заходів захисту інформації та забезпечення післягарантійного обслуговування.

РОЗДІЛ 3 РОЗРОБКА ВДОСКОНАЛЕНОЇ КСЗІ ДЛЯ ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС»

3.1 Аудит інформаційної безпеки підприємства

Аналізуючи інформацію, що циркулює в організації, дозволяється визначати, які дані потрібно захистити і як саме забезпечити її безпеку. Основною метою аналізування є виявлення будь яких джерел інформації і її носіїв, вирахування схеми конфіденційності цієї інформації.[18]

До інформації, яку необхідно захистити, відносяться конфіденційна документація. Конфіденційний документ – це правильно оформлений носій інформації яка є задокументованою, який містить обмежені відомості, доступ або використання яких обмежені, і який є інтелектуальною власністю юридичної або фізичної особи. Елементи захисту наведені у таблиці 3.1.

Таблиця 3.1 - Компоненти захисту.

№	Елемент інформації	Конфіденційність інформації	Назва джерела інформації	Місцезнаходження інформації
1	2	3	4	5
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
4	Звіти	Конфіденційно	Працівники, документи, відходи	Кабінет директора

Продовження таблиці 3.1

1	2	3	4	5

5	Фінансові звіти	Конфіденційно	Працівники, документи, відходи	Бухгалтерія
6	Податкові декларації	Конфіденційно	Працівники, документи, відходи	Бухгалтерія

Для того щоб визначити вимоги до ІС використаємо два документи: "Автоматизовані системи. Захист від НСД до ІзОД. Класифікація автоматизованих систем та вимоги щодо захисту інформації" і "Засоби обчислювальної техніки. Мережеві екрани. Захист від НСД до ІзОД. Показники захищеності від НСД до ІзОД".

Безпеці інформації загрожує можливість виникнення подій, які можуть негативно вплинути на інформацію. Ці події включають втручання до фізичного середовища та його цілісності, втручання до логічної структури, несанкціоновану модифікацію, отримання та поширення інформації. Актуальними загрозами безпеки даного підприємства є:

- відмова апаратури;

- помилкові дії чи навмисні дії персоналу інформаціонної системи;

- помилки адміністрування;

- несанкціонований доступ до інформації у місцях з необмеженим доступом;

- несанкціонований доступ до інформації через втрачання або викрадення носія;

- несанкціонований доступ до ЕОМ через цільову атаку на інформаційну систему;

- несанкціонований доступ до інформаційних ресурсів які знаходяться у паперовому вигляді в приміщеннях підприємства;

- втручання і порушення системи конфіденційності електронних документів;

- пожежі;

- втрачання чи викрадення документів;

- природні, стихійні лиха.

У таблиці 3.2 зображений макет схеми загроз і вразливостей інформаційній безпеці організації у відповідності описаним загрозам.

Таблиця 3.2 - Аналіз вразливостей підприємства

№	Загрози	Вразливості
1	2	3
1	Відмови в працездатності апаратури	- помилки операційної системи чи 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;

Продовження таблиці 3.2

1	2	3
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.

Закінчивши оцінювання загроз треба висунути пропозиції щодо методів усунення даних вразливостей. В таблиці 3.3 наведені загрози і способи їхнього усунення.

Таблиця 3.3 - Вразливості і способи їх уникнення

№	Вразливість	Метод запобігання
1	Помилки у ОС або ПЗ	- Встановлення оновлень операційної системи, програмного забезпечення, сервісних пакетів, патчів тощо - Використання перевіреного програмного забезпечення
2	Ненадійність окремих вузлів апаратури	- Контроль роботи апаратури та заміна або ремонт несправної.
3	Нестабільність електропостачання	- Використання засобів надійного електропостачання
4	Знищення електронної документації	- Застосування інструментів резервного копіювання
5	Помилки у роботі працівників внаслідок недостатньої кваліфікації	- Організація навчання персоналу - Визначення обов'язків персоналу - Процес прийому на роботу кваліфікованих спеціалістів - Моніторинг роботи персоналу
6	Навмисні дії персоналу	- Розмежування повноважень персоналу та контроль роботи персоналу
7	Необмежений доступ до інформації сторонніх осіб	- Монітори на робочих місцях розміщують так, щоб неможливо було зняти відеоінформацію з них.
8	Можливість втрати або крадіжки носія інформації	- Облік носіїв інформації здійснюється шляхом видачі їх під розпис.
9	Необмежений доступ до засобів друку та копіювання	- Контроль доступу до засобів друку.

Обробивши особисті дані в розділених інформаційних системах, які підключені до загальнодоступних мереж зв’язку та/або міжнародних мереж інформаційного обміну, можуть виникнути наступні загрози пов’язані з безпекою особистої інформації:

- Загрози витікання інформації через технічні канали;

- Загрози несанкціонованого доступу до особистих даних, які обробляються на автоматизованому робочому місці.

Загрози витоку інформації через технічні канали включають:

- Загрози витоку інформації яка належить до акустичної (мовної);

- Загрози витоку інформації яка належить до візуальної;

- Загрози витоку даних через побічні електромагнітні випромінювання.

Загрози витоку акустичних даних можуть виникнути, якщо особисті дані вводяться за допомогою мовних засобів до інформаційних систем або якщо особисті дані відтворюються акустичними засобами інформаційних систем. Загрози витоку візуальних даних можуть реалізуватися шляхом перегляду інформації на моніторах та інших засобах відображання ЕОМ, інформаційно-обчислювальних комплексів, засобів для технічної обробки графічної інформації, відеоінформації та оцифрованих текстових даних, які відносяться до складу інформаційних систем.

Небезпеки національної кібербезпеки зв’язані із атаками зловмисників, в яких є доступ до інформаційних систем, включаючи користувачів, що виконують загрози прямо в системі, а також зловмисників, які не мають доступу до системи, але реалізують загрози зовнішніми мережами спільного зв’язку.

У цих системах можуть виникати наступні загрози:

- Загрози, які виникають під час завантаження операційної системи і мають мету перехопити паролі і ідентифікатори, змінити базову систему вводу/виводу (BIOS) і перехопити управління завантаженнями.

- Загрози, пов’язані з виявленням паролів.

- Загрози, які виникають після завантаження операційної системи і спрямовані на виконання незаконних дій використовуючи стандартні функції операційної системи чи іншої допоміжного застосунку (системи керування базами даних), з використанням спеціально створених програм для отримання незаконного доступу.

- Загрози інсталювання шкідливого програмного забезпечення.

- Загрози які стосуються «аналізу сітьового трафіку» з захопленням даних, які передаються зовнішнім мережам і отримується з зовнішніх мереж.

- Загрози сканування, які розпізнають тип операційної системи, мережеву адресу робочої станції, топологію мереж, відкритого з’єднання тощо.

- Загрози отримання незаконного доступу за допомогою заміни довірених об’єктів.

- Загрози такого типу як «Відмова у обслуговуванні».

- Загрози дистанційного запускання додатків.

- Загрози того що буде нав’язування неправильного шляху, за допомогою несанкціонованої модифікації маршрутно-адресних даних які знаходяться всередині мережіта ті, що знаходяться у мережах ззовні.

Загроза вважається актуальною, якщо існує можливість її реалізації та вона представляє небезпеку. Щоб оцінити реалізацію загрози використовуються 2 показники: початковий рівень захисту і ймовірність реалізації цієї загрози. Складаючи список актуальності загроз безпеки кожному рівню початкової захищеності відповідає числовий коефіцієнт Y_1, а саме:

0 – для початкової захищеності високого рівня;

5 – для початкової захищеності середнього рівня;

10 – для початкової захищеності низького рівня.

Під ймовірністю реалізації загрози розуміється обчислювальний показник, який вказує на ймовірність виникнення конкретної загрози. Одночасно зі складанням списку актуальності загроз безпеки всім градаціям імовірності присвоюється чисельний коефіцієнт Y_2, такий як:

0 – загрозам малої імовірності;

0 – загрозам низької імовірності;

5 – загрозам середньої імовірності;

10 – загрозам високої імовірності.

З урахуванням наведеного, коефіцієнт відповідаючий реалізації загрози Y буде розраховуватись співвідношенням:

$$Y = (Y_1 + Y_2) \div 20 \quad (1)$$

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

Шанс реалізації загрози буде вважатися низьким при $0 \leq Y \leq 0{,}3$;

Шанс реалізації загрози буде вважатися середнім при $0{,}3 < Y \leq 0{,}6$;

Шанс реалізації загрози буде вважатися високим при $0{,}6 < Y \leq 0{,}8$;

Шанс реалізації загрози буде вважатися дуже високим при $Y > 0{,}8$.

Таблиця 3.4 – Модель загроз

№	Загроза	Y2	Y	Можливість реалізації загрози	Небезпека	Актуальність
1	2	3	4	5	6	7
1	Загроза витоку акустичної інформації	0	0.25	низька	низька	неактуальна
2	Загрози витоку візуальної інформації	2	0.35	середня	низька	неактуальна
3	Загрози, спрямовані на перехоплення паролів,	5	0.5	середня	середня	актуальна

	модифікацію базової системи введення/виведення, перехоплення керування завантаженням.					

Продовження таблиці 3.4

1	2	3	4	5	6	7
4	Загрози виявлення паролів	5	0.5	середня	середня	актуальна
5	Загрози, спрямовані на отримання НСД за допомогою стандартних функцій операційної системи або будь-якої програми за допомогою спеціально створених для цього програм.	5	0.5	середня	висока	актуальна
6	Загроза впровадження шкідливого ПЗ	5	0.5	висока	висока	актуальна
7	Сканування загроз, спрямоване на виявлення типу операційної системи, 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

Кінець таблиці 3.4

1	2	3	4	5	6	7

11	Небезпека неправильного маршруту через несанкціоновану зміну маршрутно-адресних даних.	2	0.35	низька	низька	неактуальна

3.2 Вимоги до створення КСЗІ

Аудит інформаційних систем об’єкта, що захищається, виявив, що важливі дані широко поширені всередині організації. За результатами аудиту інформаційних систем було сформовано вичерпний список існуючих ризиків безпеки. Для створення надійної системи захисту інформації вкрай важливо запропонувати ефективні заходи протидії цим загрозам. Ці методи повинні випливати із законів України, федеральних законів, нормативно-правових актів, постанов і розпоряджень Уряду України. Механізми захисту, що використовуються в системах захисту, повинні бути взаємопов’язані між різними місцями, часовими рамками та конкретними діями, на які вони спрямовані. Комплексність охоплює використання різноманітних методів і підходів до захисту інформації, включаючи організаційні, технічні, програмні, криптографічні та правові заходи. Система захисту повинна складатися з декількох шарів, які перетинаються один з одним. Метою інженерно-технічних заходів є недопущення сторонніх осіб до офісних приміщень, доступу до інформаційних систем, обмеження дій користувачів.

За забезпечення конфіденційності, цілісності та доступності інформації, що обробляється, відповідає система безпеки, яка поєднує програмне та апаратне забезпечення. Щоб захистити інформацію, організації впроваджують практики та процедури, яких мають дотримуватися уповноважені особи під час обробки інформації, забезпечуючи заздалегідь визначений рівень безпеки. Для забезпечення захисту конфіденційної інформації організації повинні мати не тільки документи, пов’язані з їхньою роботою з конфіденційними даними, але й

документи, які створюють систему безпечного обігу захищених документів у системі електронного документообігу.[19]

3.3 Програмно-апаратний захист підприємства

На об’єкті, що охороняється, відеокамери повинні бути стратегічно розташовані в місцях, куди можуть проникнути зловмисники, а також у місцях, де можна спостерігати відвідувачів, які пересуваються по коридору. Камери повинні бути стратегічно розташовані, щоб забезпечити постійний контроль за пожежними виходами, ліфтами, коридорами та входами до будівлі. Зовнішні відеокамери стратегічно розташовані по периметру закладу, щоб запобігти розміщенню зловмисниками неавторизованих апаратних пристроїв за межами приміщення.

Була обрана вулична кольорова відеокамера Hikvision DS-2CD2143G0-I з ринку телевізійних відеокамер. Ця камера є купольною мережевою IP-камерою з високою роздільною здатністю і підходить для використання як всередині приміщень, так і на відкритому повітрі. Вона має багато функцій, які забезпечують високу якість відеоспостереження та надійність в різних умовах.

Основні характеристики цієї камери включають:

1. Роздільна здатність 4 мегапікселі, що дозволяє отримувати чіткі та деталізовані зображення.

2. Інфрачервоне підсвічування (IR) до 30 метрів нічного бачення, що забезпечує видимість навіть у повній темряві.

3. Підтримка стиснення відео H.265+, H.265, H.264+, H.264 для ефективного використання дискового простору.

4. Ступінь захисту IP67, що робить камеру стійкою до пилу та води.

5. Ступінь захисту IK10, що забезпечує стійкість до механічних пошкоджень.

6. Інтелектуальні функції, такі як виявлення руху, лінійне перетинання, виявлення вторгнень та інші функції аналізу відео.

7. Підтримка Power over Ethernet (PoE), що спрощує установку і зменшує кількість необхідних кабелів.

Ця камера повністю відповідає вимогам щодо кута огляду для всіх зон спостереження як всередині, так і ззовні об'єкта захисту.

Функції поста керування на об’єкті виконується в приміщенні, яке знаходиться на першому поверсі будівлі. На цьому посту керування повинен постійно присутній охоронець. У цьому приміщенні також розташовані сервер відеоспостереження з монітором та засіб охоронно-пожежної сигналізації, який працює в парі з модулем спостереження та керування.

Щоб гарантувати безпеку даних від шкідливого програмного забезпечення на всіх робочих станціях і корпоративному сервері, дуже важливо встановити антивірусні програми, які автоматично оновлюють свої антивірусні бази даних з локального дзеркала, розташованого на сервері.

Symantec Endpoint Protection (SEP), розроблений компанією Symantec (тепер частина Broadcom), є потужним антивірусним рішенням для захисту ендпоінтів. Цей продукт спрямований на забезпечення безпеки комп'ютерів, серверів та мобільних пристроїв від широкого спектру загроз.

Основні характеристики Symantec Endpoint Protection як антивірусу:

1. Антивірусний захист**:**

SEP виявляє та видаляє віруси, трояни, руткіти, шпигунські програми та інші шкідливі програми за допомогою баз даних вірусних сигнатур.

Вірусні бази даних регулярно оновлюються, забезпечуючи захист від нових загроз.

2. Проактивні технології захисту**:**

SEP використовує евристичний аналіз для виявлення нових, невідомих загроз шляхом аналізу поведінки програм.

Технологія SONAR аналізує поведінку програм у реальному часі для виявлення підозрілої активності та невідомих загроз.

3. Розширені можливості сканування**:**

SEP пропонує як повне сканування системи, так і інкрементальне сканування, яке перевіряє лише нові або змінені файли, знижуючи навантаження на систему.

Можливість налаштування автоматичного сканування за розкладом для регулярної перевірки системи на наявність загроз.

4. Реальний час захисту**:**

SEP забезпечує постійний моніторинг файлів і процесів на пристрої, миттєво реагуючи на виявлення шкідливого ПЗ.

5. Легка інтеграція та управління**:**

Адміністратори можуть централізовано керувати всіма налаштуваннями та політиками безпеки через консоль Symantec Endpoint Protection Manager (SEPM).

Зручний інтерфейс дозволяє легко налаштовувати параметри захисту та переглядати звіти про стан безпеки.

6. Захист від мережевих загроз**:**

Вбудований фаєрвол і система запобігання вторгненням (IPS) захищають від мережевих атак, забезпечуючи додатковий рівень захисту.

Symantec Endpoint Protection икористовує сучасні технології аналізу та виявлення загроз, що забезпечує високий рівень захисту. Має оптимізовані алгоритми сканування зменшують навантаження на систему, що дозволяє користувачам працювати без помітних знижених швидкодій. Гнучкі параметри налаштування дозволяють адаптувати захист під конкретні потреби організації.

Однією з важливих задач при експлуатації інформаційних систем є забезпечення цілісності даних, тому необхідно мати механізм для швидкого відновлення втрачених даних. Для цього можна побудувати розвинену систему

резервного копіювання, яка періодично створює копії інформації з метою подальшого відновлення в разі часткового або повного руйнування.

Система резервного копіювання повинна відповідати наступним вимогам:

- використання технології «клієнт-сервер» для мережевого резервного копіювання;

- автоматизація процесу резервного копіювання;

- використання надійного носія для зберігання резервних копій;

- верифікація та стиснення інформації;

- швидке відновлення серверів після аварії;

- резервне копіювання баз даних у реальному часі;

- підтримка різноманітних середовищ;

- ефективні засоби управління та моніторингу.

Програмне забезпечення Veeam Backup & Replication відповідає цим вимогам. Цей продукт призначений для підприємств будь-якого розміру, здатний зростати разом з компанією і легко масштабується від локальних конфігурацій до великих територіально розподілених мереж з тисячами машин.[15] Veeam Backup & Replication надає організаціям розширені можливості резервного копіювання та відновлення системи, включаючи дедуплікацію даних, підвищену безпеку та панель моніторингу операцій.

Основні переваги Veeam Backup & Replication включають:

1. Швидке і надійне відновлення.

2. Централізована панель моніторингу, яка керує процесами резервного копіювання та відновлення всіх робочих станцій та серверів і надає інформацію про виконувані або заплановані завдання.

3. Дедублікація на рівні файлів та блоків, що уникне повторного резервного копіювання одних і тих же даних і зменшить витрати на передачу та зберігання резервних копій.

4. Групування завдань за допомогою політик резервного копіювання та відновлення дозволяє автоматизувати схожі дії.

Технологія IP стверджує, що вона може керувати потоком інформації завдяки взаємозалежному управлінню потоками трафіку, що уможливлює використання IP. Ця технологія передачі даних використовує протокол IP-тунелювання, який дозволяє інкапсулювати один IP-пакет в інший IP-пакет. При цьому, в зовнішньому пакеті додається заголовок зі значеннями SourceIP (точка входу в тунель) і Destination (точка виходу з тунелю), а внутрішній пакет залишається без змін, за винятком поля TTL, яке зменшується. Поля "Do not Fragment" і "The Type of Service" повинні бути скопійовані в зовнішній пакет. Якщо розмір пакета перевищує Path MTU, пакет буде поділено в інкапсуляторі, за винятком включень у зовнішній заголовок. Пакет який повинен бути видалений, видаляється декапсулятором в останній момент. Змінити кількість активних політик IPsec можна за допомогою мережевого тунелю. Фрагменти тунелю призначені для інкапсуляції трафіку, а деякі маршрути можуть реєструвати дві адреси в політиках IPsec, щоб запобігти плутанині. Шифрування IPsec є надійним засобом підвищення безпеки, але в даний час це найбільш ефективний метод забезпечення захисту та безпеки даних. Шифрування дозволяє перехоплювати дані по тунелю тунелю, щоб зловмисник не зміг їх прочитати або вкрасти.

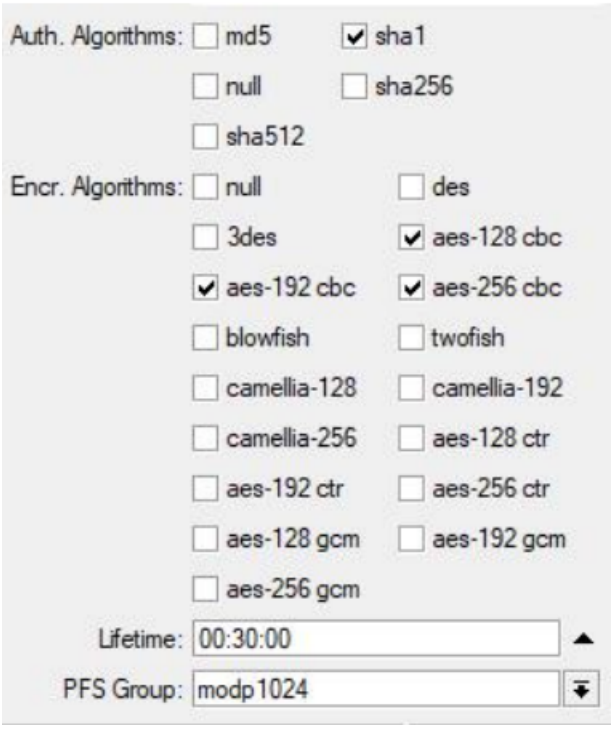

Рисунок 3.1 - Шифрування трафіку в IPsec

3.4 Фізичний захист інформації

Всі способи, що відрізняються від фізичної присутності на об'єкті, що охороняється для доступу до інформації до фізичного доступу до інформації, розглядаються раніше і включають всі способи, що включають фізичний доступ до володіння інформацією і фізична присутність на об'єкті, що охороняється.

Спочатку слід вказати вимоги до кімнати, де проводяться всі наради, на яких обговорюється важлива інформація. В основу цієї кімнати, що є закритою областю, створеною з електропровідного матеріалу, лягла концепція клітини Фарадея, заснована на концепції сітки або цілісних елементів. Клітина Фарадея характеризується зовнішніми статичними та динамічними електричними полями, які нейтралізуються нейтралізацією електричних полів клітиною Фарадея, що робить практично непрактичним передачу та прийом радіохвиль за допомогою антени, розташованої в клітині Фарадея. Клітина блокує або сильно

послаблює сигнал повністю блокуючи його. При створенні кліток Фарадея можуть бути використані різні типи матеріалів, такі як:

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

Стінки кімнати, де проводяться наради, повинні бути подвійними з обов'язковим повітряним шаром між ними. Це рішення перешкоджає отриманню інформації за допомогою спеціальних пристроїв, які зчитують вібрації і перетворюють їх на текстову інформацію.

Щоб забезпечити безпеку об'єкту, необхідно провести серйозні заходи на всій його території. На всіх вікнах повинні бути встановлені решітки, щоб унеможливити проникнення зловмисників через них. Також на вікнах слід встановити спеціальні пристрої, які створюють вібрацію, щоб запобігти дистанційному отриманню важливої інформації зловмисниками за допомогою спеціального технічного обладнання. При покиданні працівниками об'єкту всі вікна повинні бути зачиненими, щоб унеможливити можливість зловмисників підкинути звукозаписуючий пристрій з можливістю дистанційної передачі інформації.

Всі сервери повинні бути розміщені у спеціально обладнаних кімнатах з обмеженим доступом. У наш час вже є пристрої, які можуть зчитувати інформацію з серверів, аналізуючи звук роботи вентилятора, що відповідає за їх охолодження. Це означає, що необхідно будувати кімнату, враховуючи можливість зловмиснику мати доступ до вентилятора охолодження. У цій кімнаті мають бути розташовані усі сервери, включаючи ті, що містять резервні

копії інформації. Дозволяється залишити тестовий сервер для проведення випробувань нових методів захисту програмної інформації.

3.5 Організаційний захист інформації

Захист інформації в організації - це сукупність способів і правил, які вказують, як забезпечувати безпеку інформації та підтримувати персонал у дотриманні конфіденційності даних.[20]

Організаційні методи - це основа для комплексної системи захисту підприємства. Лише завдяки цим методам можна всі заходи захисту поєднати в єдину систему.

Основні організаційні заходи із захисту інформації на об'єкті включають:

1. Створення структури служби безпеки та організацію режиму та охорони.

2. Організація внутрішньооб'єктного режиму та охорони об'єктів підприємства.

3. Підбір та навчання персоналу, перевірка їх надійності, укладання угод, навчання правилам роботи з конфіденційною інформацією та ознайомлення з відповідальністю за порушення правил захисту інформації.

4. Організація роботи з документами та документованою інформацією, включаючи розробку і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання та знищення.

5. Організація роботи з електронними документами та інформаційною системою підприємства, включаючи роботу в локальній обчислювальній мережі і правила доступу до мережі Інтернет.

6. Систематичний контроль роботи персоналу з конфіденційною інформацією, облік, зберігання та знищення документів і технічних носіїв.

7. Організація роботи з відвідувачами під час нарад і переговорів.

8. Інформаційно-аналітична робота, що включає аналіз і накопичення інформації з елементами прогнозування з питань, що стосуються безпеки керування і підготовку рекомендацій керівництву щодо правомірного захисту.

До методів організаційного захисту інформації слід віднести розмежування доступу до неї. Наразі доступ до неї має кожен системний адміністратор. Це створює ризик отримання несанкціонованого доступу до інформації шляхом отримання доступу до робочого місця одного з адміністраторів. Для запобігання цій загрозі необхідно дозволити лише одній людині у відділі мати доступ до інформації та максимально захистити її робочу станцію.

Також слід проводити щомісяця заходи з метою пошуку програмно-апаратних закладних пристроїв. Останнім часом збільшується кількість комплексних атак, які використовують різноманітні програми та пристрої. Підготовка до таких атак може зайняти від двох місяців до півроку, тому необхідно щомісяця проводити пошук признаків планованої атаки та нейтралізувати всі виявлені пристрої та програми.

ВИСНОВКИ

1. В даній кваліфікаційній роботі було проаналізовано сфери інформації, які повинні захищати КСЗІ, виконано їх загальний огляд, та проблем, що вона вирішує. Також розглянуто методи створення КСЗІ на підприємстві.

2. Проведено дослідження існуючих рішень КСЗІ. Докладно досліджено комплексні системи захисту інформації, такі як “ Symantec Integrated Cyber Defense ” та “ Fortinet Security Fabric ”. Розглянуто їхні можливості, функціонал та вимоги. Окрему увагу приділено аналізу компонентів, що входять до складу зазначених систем захисту інформації. Важливо пам'ятати, що існує можливість покращення КСЗІ шляхом додавання різноманітних ПАК, встановлення різноманітних додаткових програм, таких як системи IDS та IPS, а також додавання технічного обладнання, наприклад серверів та мережевих екранів.

3. Розроблено алгоритм створення комплексної системи захисту інформації на прикладі ТОВ «ААЗ ТРЕЙДІНГ-АВТОЛЮКС».Проведено дослідження послідовності етапів створення КСЗІ, а також питання, документи, що розглядаються та створюються на кожному етапі. Окремо вивчено процес розробки політики безпеки підприємства, а також необхідні елементи, які вона повинна містити. Представлено документи та стандарти, яким має відповідати комплексна система захисту інформації (КСЗІ). Якщо система не відповідає хоча б одній нормі, компанія або підприємство не зможуть отримати атестат, що вказуватиме на незахищеність інформаційної системи компанії або підприємства.

4. Після проведення детального аудиту, необхідності впровадження комплексної системи захисту інформації (КСЗІ) на підприємстві, рівня конфіденційності обігу даних та документів запропоновано покращення та вдосконалення системи захисту інформації. Визначено ключові області захисту,

потенційні ризики та загрози, що можуть призвести до несанкціонованого доступу до інформації (НСД), крадіжки даних або втрат через стихійні лиха. Створено персоналізовану таблицю ризиків та запропоновано методи їх уникнення. Також розроблено таблицю актуальності питань захисту від втрат або несанкціонованого доступу до інформації. Надано рекомендації щодо апаратного та програмного забезпечення для впровадження КСЗІ на підприємстві.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ДСТУ 3396.1-96 Захист інформації Технічний захист інформації. Порядок проведення робіт. [Чинний від 01.07.1997 р.] Київ: Державна служба спеціального зв'язку та захисту інформації України, 1996, 11 с.

2. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованих системах, наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.4-001-2000.pdf

3. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2, наказ ДСТСЗІ СБУ від 13.12.2002 № 84 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-008-2002.pdf

4. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 02.04.2003 № 33 (Зміна № 1 наказ від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-010-03.pdf

5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-002-99.pdf

6. НД ТЗІ 1.6-002-2003 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації, наказ ДСТСЗІ СБУ від 24.04.2003 № 41 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск., зміна № 2, наказ Адміністрації

Держспецзв'язку від 17.08.2013 № 451) [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/services/cm/api/attachment/download?id=53374

7. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ ДСТСЗІ СБУ від 18.06.2002 № 37, зміна № 2 наказ Адміністрації Держспецзв'язку від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-001-99.pdf

8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806) [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-004-99.pdf

9. ТР ЕОТ -95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок, наказ Державної служби України з питань ТЗІ від 09.06.95 № 25 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск) [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/services/cm/api/attachment/download?id=53372

10. ТР ТЗІ – ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок, наказ ДСТЗІ від 09.06.95 № 25, наказ Державної служби України з питань ТЗІ від 09.06.95 № 25 (Зміна № 1, наказ Адміністрації Держспецзв'язку від 03.11.2011 № 93 дск) [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/services/cm/api/attachment/download?id=53373

11. Integrated Cyber Defense Essential Security Solutions Working Together to Protect Your Business [Електронний ресурс] — Режим доступу до ресурсу:

https://cyberedgegroup.com/wp-content/uploads/2021/05/Symantec-Integrated-Cyber-Defense-White-Paper.pdf

12. Fortinet Whitepaper — Building a Security Fabric for Today's Network [Електронний ресурс] — Режим доступу до ресурсу: https://broadviewnetworks.ca/wp-content/uploads/2018/02/whitepaper-fortinet-building-security-fabric-for-todays-network.pdf

13. Гребенніков В.В. — Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій. 2013. 161 с. [Електронний ресурс] — Режим доступу до ресурсу: https://www.academia.edu/40525032/Комплексні_системи_захисту_інформації_проектування_впровадження_супровід

14. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет [Електронний ресурс] — Режим доступу до ресурсу: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet?fbclid=IwAR3RcWOpnttuJROqWpz0bwL1u0OsySollvFJqw2vLCFk6X_EA79Se3_1ZY

15. VEEAM BACKUP & REPLICATION Secure Backup, Clean Recovery and Data Resilience – Delivered Instantly [Електронний ресурс] — Режим доступу до ресурсу: https://www.veeam.com/products/veeam-data-platform/backup-recovery.html

16. Демуз І. О. Документаційне забезпечення діяльності державних установ навч.-мет. посіб. Переяслав-Хмельницький : Домбровська Я. М., 2018. 210 с.

17. Закон України «Про внесення змін до законів України щодо інформаційної безпеки» [Електронний ресурс] – Режим доступу до ресурсу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH77G00A.html

18. Аль-Амморі А.Н., Зозуля Н.Ю., Наумова Н.М. Інформаційно-аналітична діяльність : навч. посіб. для студентів вищих навчальних закладів. Київ : НТУ, 2018. 146 с.

19. НК 010:2021. Класифікатор управлінської документації. Київ : Український науково-дослідний інститут архівної справи та документознавства, 2021. 26 с.

20. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.