МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «АНАЛІЗ МЕТОДІВ ІНЦИДЕНТНОГО РЕАГУВАННЯ ТА ВІДНОВЛЕННЯ ПІСЛЯ КІБЕРАТАКИ В КОРПОРАТИВНИХ МЕРЕЖАХ»

на здобуття освітнього ступеня бакалавра

зі спеціальності 125 Кібербезпека

освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ганна САВЕНОК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБЗ-51

САВЕНОК Ганна

Керівник: ПОРОХНИЦЬКИЙ Олександр
(ПРІЗВИЩЕ, Ім'я)

Рецензент: КОТЕНКО Андрій
к.т.н., доцент (ПРІЗВИЩ Е, Ім'я

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти бакалавр
Спеціальність Кібербезпека
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ

_____ Світлана ЛЕГОМІНОВА
«____» _____ 2024 р

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Савенок Ганна Юріївна
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: «Аналіз методів інцидентного реагування та відновлення після кібератаки в корпоративних мережах»
керівник кваліфікаційної роботи Олександр ПОРОХНИЦЬКИЙ
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

затверджена наказом Державного університету інформаційно-комунікаційних технологій від "27" лютого 2024 р. № 36.

2. Строк подання кваліфікаційної роботи 20.05.2024 р

3. Вихідні дані до кваліфікаційної роботи: об'єкт інформаційної діяльності, корпоративна мережа передачі корисних даних, вимоги до захисту корпоративної інформації в мережах передачі даних.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Провести аналіз процесу кібератаки та визначити поняття загроз інформаційної безпеки в корпоративних мережах;
4.2. Проаналізувати механізми реалізації та провести класифікацію кібер загроз та кібератак на корпоративні мережі;
4.3. Розробити методи та практичні рекомендацій що до захисту від кібератаки в корпоративних мережах.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.02.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2024	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	22.04.2024	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	13.06.2024	

Здобувач вищої освіти _____ Ганна САВЕНОК
(підпис) (Ім’я, ПРІЗВИЩЕ)

Керівник роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

Направляється здобувач(ка) *Савенок Г.Ю.* до захисту кваліфікаційної роботи
……(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

освітньо-професійної програми «Інформаційна та кібернетична безпека»
(назва)
на тему: «Аналіз методів інцидентного реагування та відновлення після кібератаки в корпоративних мережах»

Директор ННІЗІ _____ Віталій САВЧЕНКО
... .(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач (ка) Савенок Ганна Юріївна виконала кваліфікаційну роботу, направлену на вирішення актуальної задачі – є підвищення ефективності захисту корпоративних мереж в умовах впливу спрямованих кібератак. Робота представляє науковий та практичний інтерес, всі подані основні положення є теоретично обґрунтованими, їй властива внутрішня єдність. Робота написана зрозумілою мовою, стиль викладення матеріалу забезпечує доступність його сприйняття. Дипломник проявила старанність і сумлінність в роботі, продемонстрував компетентність та здібність аналізувати і вирішувати складні задачі, має нахил до науково-дослідницької роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***САВЕНОК Ганни*** на оцінку **"добре"** та присвоїти їй кваліфікацію бакалавр з кібербезпеки за освітньою програмою «Інформаційна та кібернетична безпека»

Керівник кваліфікаційної роботи _____ Олександр ПОРОХНИЦЬКИЙ
(підпис) *(ім'я, прізвище)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) *Савенок Г.Ю.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління інформаційною та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(назва) (підпис) (Ім'я, ПРІЗВИЩЕ)

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня бакалавр здобувача вищої освіти

Савенок Ганна Юріївна

(прізвище, ім'я, по батькові)

на тему «Аналіз методів інцидентного реагування та відновлення після кібератаки в корпоративних мережах»

Актуальність.

Організація, як об'єкт інформаційної діяльності зобов'язана створити систему захисту конфіденційної інформації, котра унеможливить несанкціонований доступ до неї. Організація, з урахуванням особливостей діяльності, згідно складу конфіденційної інформації, необхідно розробити та затвердити переліки конкретних видів документів, котрі містять інформацію, положення про конфіденційну інформацію, інструкцію з роботи з документами, які містять конфіденційну інформацію та інше.

Перелік та обсяг відомостей, котрі належать до конфіденційної інформації, терміни конфіденційності, порядок захисту та доступу, правила їх застосування визначає керівник організації..

Позитивні сторони.

1) – Проаналізовано систему забезпечення та технології інформаційної безпеки корпоративних мереж організації;
2) – Досліджено процеси забезпечення та технології захисту конфіденційної інформації;
3) – Розроблені методи забезпечення захисту конфіденційної інформації в корпоративних мережах організації.

Недоліки.

1. У роботі є деякі помилки стосовно оформлення.
2. В роботі аналіз об'єкта інформаційної діяльності проведено відносно найбільш відомих каналів витоку інформації, хоча в галузу захисту інформації відомий більш широкий перелік таких каналів та каналів доступу до процесів передачі даних через телекомунікаційні мережі.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"_____"**, а здобувач(ка) **САВЕНОК Ганна** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Рецензент: _____ Андрій КОТЕНКО
к.т.н., доцент *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 70 сторінки. Список використаних джерел містить 37 найменувань і займає 4 сторінки.

Ключовими методами аналізу стану забезпечення інформаційної безпеки корпоративної мережі є описи методів та їх класифікації. Щоб здійснити ефективний захист корпоративної мережі, варто описати процес, а далі здійснити класифікацію методів відповідно до видів загроз та небезпек, ризиків та викликів для інформаційної безпеки, згідно підготовки системи заходів для керування ними.

В кваліфікаційній роботі проведено аналіз методів та засобів, які спрямовані на підвищення захисту корпоративних мереж від спрямованих кібератак.

Метою кваліфікаційної роботи є підвищення ефективності захисту корпоративних мереж в умовах впливу спрямованих кібератак.

Об'єкт дослідження. Корпоративна мережа передачі даних.

Предмет дослідження. Методи захисту корпоративної мережі від мережевих загроз.

У кваліфікаційній роботі були вирішені наступні завдання:

– визначені поняття загроз інформаційної безпеки в корпоративних мережах

– проведено класифікацію загроз та атак на корпоративні мережі.

– розроблено методи захисту від кібератаки в корпоративних мережах.

Практична цінність. Результати досліджень можна використовувати для підвищення ефективності захисту корпоративної мережі від кібератак.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖЕВІ ЗАГРОЗИ, ПРОТОКОЛИ ЗАХИСТУ, ІНЦИДЕНТНЕ РЕАГУВАННЯ.

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of used sources, the total volume of the work is 70 pages. The list of used sources contains 37 names and occupies 4 pages.

Descriptions of methods and their classification are key methods of analyzing the state of information security of a corporate network. In order to carry out effective protection of the corporate network, it is necessary to describe the process, and then to carry out the classification of methods according to the types of threats and dangers, risks and challenges for information security, according to the preparation of a system of measures to manage them.

In the qualification work, an analysis of methods and means aimed at increasing the protection of corporate networks from targeted cyber attacks was carried out.

The purpose of the qualification work is to research the methods of protecting corporate networks under the influence of targeted cyber attacks.

Object of study. Corporate data transmission network.

Subject of study. Methods of protection against network threats in the corporate network.

The following tasks were solved in the qualification work:

- defined concepts of threats to information security in corporate networks

– classification of threats and attacks on corporate networks was carried out.

- developed methods of protection against cyber attacks in corporate networks.

Practical value. Research results can be used to improve the effectiveness of corporate network protection against cyber attacks.

Keywords: INFORMATION SECURITY, NETWORK THREATS, PROTECTION PROTOCOLS, INCIDENT RESPONSE.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AH	–	Authentication Heade
DLPS	–	Data Loss Prevention Systems
ESP	–	Electronic Stability Program
FTP	–	File Transfer Protocol
HTTP	–	HyperText Transfer Protocol
ICMP	–	Internet Control Message Protocol
IKE	–	Internet Key Exchange
IPS	–	Intrusion Prevention Systems
IPSec	–	IPSec Internet Protocol Security
IRC	–	Internet Relay Chat
ISAKMP	–	Internet Security Association and Key Management Protocol
OTP	–	OneTime Passwords
SA	–	Security Association
TCP	–	Transmission Control Protocol
TLS	–	Transport layer security
UDP	–	User Datagram Protocol
VPN	–	Virtual Private Network
ОС	–	Операційна система
ПЗ	–	Програмне забезпечення
СУБД	–	Система управління базою даних

ВСТУП

Задля забезпечення інформаційної безпеки установи та організації підрозділи технічного захисту інформації вдаються до застосування способів, засобів та прийомів, які включають методи кіберзахисту корпоративних мереж від спрямованих кібератак. Методи передбачають собою деяку послідовність подій, які ґрунтуються на конкретному плані. Вони можуть модифікуватися чи вдосконалюватися, допрацьовавуватися та варіюватися у залежності від типу діяльності, де застосуються та використовуються [8].

Ключовими методами аналізу стану забезпечення інформаційної безпеки корпоративної мережі є описи методів та їх класифікації. Щоб здійснити ефективний захист корпоративної мережі, варто описати процес, а далі здійснити класифікацію методів відповідно до видів загроз та небезпек, ризиків та викликів для інформаційної безпеки, згідно підготовки системи заходів для керування ними [8].

Для розповсюджених методів аналізу рівня забезпечення інформаційної безпеки на об’єкті інформаційної діяльності, застосовуються методи дослідження зв’язків [8].

Завдяки застосовуваних методів [8]:

- виявляються причинно-наслідкові зв’язки між загрозами та небезпеками;
- здійснюється пошук причин, які спровокували небезпеку та поновлення чинників небезпеки;
- розробляються заходи з ліквідацією та нейтралізації небезпек.

Методи причинно-наслідкових зв’язків є [5]:

- метод схожості;
- метод розбіжності;
- метод поєднання схожості та розбіжності;
- метод супроводжувальних змін;
- метод залишків.

Вибір методів аналізу ситуації щодо забезпечення інформаційної безпеки на об’єкті інформаційної діяльності у залежності від певного рівня та сфери діяльності організації щодо захисту. У залежності від загрози ускладнюється задача для диференціації рівнів загроз та рівнів захисту. Якщо говорити про сфери інформаційної безпеки, то у ній виокремлюють, які розглянемо та деталізуємо у розділі роботи [5]:

1) фізичний;

2) програмно-технічний;

3) управлінський;

4) технологічний;

5) рівень користувача;

6) мережевий;

7) процедурний.

Наразі відбувається швидкий розвиток інформаційних технологій, і вони з’являються у кожній сфері нашого життя, застосовуються у будь-якій діяльності, це нажаль призводить до зростання кількості шахрайств та злочинів, які направлені на інформаційну безпеку. Кіберзлочинці знаходяться постійно у пошуку нових вразливостей систем, особливо їх увагу привертає діяльність державних структур та комерційних підприємств. Мета кіберзлочинців є розкрадання, розголошення конфіденційної інформації, підрив репутації, порушення нормального режиму роботи та доступ до інформаційних ресурсів об’єкту інформаційної діяльності. Такі дії завдають моральних та матеріальних збитків, тому дана тема є **актуальною**.

Ризики можуть бути не лише для великих організацій, але й для конкретних користувачів, так як саме вони більше нехтують своєю безпекою. Завдяки засобів шахраї отримують доступ до персональних даних (наприклад, номерів банківських рахунків, кредитних карт, паролів, виведення обчислювальних систем з ладу чи отримують доступ до комп’ютера чи телефону). Після зараження застосовуються дані пристрої зловмисниками для

здійснення атак на сервери, розсилки спаму, збору конфіденційної інформації, розповсюдження нових вірусів та троянських програм [5].

Метою роботи є підвищення ефективності захисту корпоративних мереж в умовах впливу спрямованих кібератак.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі**:

1. Визначення поняття загроз інформаційної безпеки в корпоративних мережах

2. Класифікація загроз та атак на корпоративні мережі.

3. Розробка методів захисту від кібератаки в корпоративних мережах.

Об'єкт дослідження. Корпоративна мережа передачі даних.

Предмет дослідження. Методи захисту від мережевих загроз в корпоративній мережі.

Практична цінність. Результати досліджень можна використовувати для підвищення ефективності захисту корпоративної мережі від кібератак.

Розділ 1 ПОНЯТТЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Аналіз порушень інформаційної безпеки

У сфері інформаційної безпеки виокремлюють наступні рівні забезпечення мережевого захисту [20]:

- фізичний;

Йому притаманна організація та фізичний захист інформаційних ресурсів та технологій, які застосовуються та управлінські технології.

- програмно-технічний;

Йому притаманна ідентифікація та перевірка дійсності користувачів, керування доступом, протоколювання та аудит, криптографія, екранування, забезпечення високого рівня доступності.

- управлінський;

Йому притаманне управління, координація іта контроль організаційних та технічних заходів на рівнях зі сторони забезпечення інформаційної безпеки на об’єкті інформаційної діяльності.

- технологічний;

Йому притаманна реалізація політики інформаційної безпеки завдяки використання комплексу сучасних автоматизованих технологій інформаційної безпеки.

- рівень користувача;

Йому притаманна реалізація політики інформаційної безпеки, яка направлена на зменшення впливу на об’єкти інформаційної діяльності, за для зниження та зменшення впливу зі сторони зовнішнього середовища.

- мережевий;

Йому притаманна реалізація у форматі координації дій та компонентів системи управління, котрі зв’язані між собою.

- процедурний.

Йому притаманне впровадження заходів, які здійснюються людьми. Заходи поділяються на групи: управління користувачами, фізичний захист, підтримка роботи системи, здійснення заходів у випадку порушення режиму безпеки, планування відновлювальних робіт.

Типи методів для забезпечення інформаційної безпеки на об’єкті інформаційної діяльності включають наступні [20]:

- однорівневими методами є ті, які ґрунтуються на підставі одного принципу управління інформаційною безпекою;
- багаторівневими методами, вважаються ті, як ґрунтуються на основі кількох принципів управління інформаційною безпекою, де кожен з них займається вирішенням конкретного питання чи проблеми. Приватні технології не зв’язані між собою та направлені на конкретні чинники інформаційних загроз;
- комплексними методами, вважаються ті, які є багаторівневими та пов’язані між собою у єдину систему, де координуючими функціями виступають на організаційному рівні для забезпечення інформаційної безпеки, аналізуючи сукупність чинників небезпеки, котрі пов’язуються семантичним зв’язком чи генеруються;
- інтегрованими високоінтелектуальними методами, вважаються ті, які є багаторівневими, багатокомпонентними технологіями, які ґрунтуються на могутніх автоматизованих інтелектуальних засобах з організаційним управлінням.

Загальними методами задля забезпечення інформаційної безпеки, досить активно застосовується на будь-якій стадії керування загроз [20].

Такими стадіями є [32]:

- рішення приймаються для виявлення області та контексту інформаційної загрози та склад учасників процесу протидії;
- схвалення стратегії та подій у різних сферах життєдіяльності;
- сприйняття загроз та небезпек в рівнях, які знаходяться нижче за організаційні ланки системи управління;
- виявлення певних політичних, економічних, соціальних,

адміністративних та організаційних ресурсів, які необхідні для запобігання загроз інформаційної безпеки;

- збереження розвитку інформаційних ресурсів системи управління.

Методи, які використовуються є специфічними та залежать від суб'єкта діяльності, об'єкта впливу [32].

Умовами щодо забезпечення інформаційної безпеки є конфіденційність, доступність, цілісність, захист інформації від існуючих та потенційних загроз. Тому, система, котра буде застосовуватися має реагувати та гарантувати ефективність її застосування [32].

Задачею захисту для забезпечення постійності та захисту від модифікації інформації у процесі збереження чи передачі інформації, мається на увазі цілісність. Конфіденційність інформації, котра забезпечується завдяки криптографічних методів, які являються не головною метою для проектування систем захисту інформації. Здійснення процедур криптографічного кодування та розкодування, що знижує швидкість передачі даних та доступу до них через те, а користувач при цьому позбавляється можливості своєчасного та швидкого доступу до необхідних даних та інформації [22].

Забезпечення конфіденційності інформації має відповідати рівню доступу до неї. Керування у сфері інформаційної безпеки має реалізовуватися на основі принципу доступності та безпеки. Система із забезпечення інформаційної безпеки перш за все, має забезпечувати доступність, цілісність та конфіденційність інформації [22].

Ато варто зауважити, що створивши та впровадивши систему інформаційної безпеки, очікувати від неї стовідсоткового захисту не можна, так як вона не є досконалою, і загрози повсюду, і їх наявність є природним компонентом системи інформаційної безпеки. І це дає змогу зрозуміти, які саме недоліки оточують системи та дають поштовх до вдосконалення чи розвитку. Тому, для об'єкту інформації діяльності, необхідно звернути увагу на методи розвитку, котрі застосовуються [22].

Захист інформації має включати у собі не лише з технічних методів для ефективного захисту інформаційної безпеки. Моделі, методи оцінки та небезпеки залежать від рівня розвитку, контексту оцінки, які застосовуються, наявність даних за факторами загроз та розмір наслідків [34].

Головним методом щодо аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз тощо. Мета якісної оцінки ризиків є – ранжування інформаційних загроз та небезпек за певними характеристиками, де система дозволяє сформулювати систему впливу [34].

Метод для забезпечення інформаційної безпеки на об’єкті інформаційної діяльності це є метод критичних сценаріїв, де здійснюється аналіз ситуації та може знизити здатність для підтримки керування в межах оптимальних параметрів. Аналіз подій може наштовхнути на той факт, що інформаційні війни є невід’ємною частиною політики безпеки [34].

Метод моделювання завдяки здійснення навчання з інформаційної безпеки. Перспективним досвідом, це є база певної американської корпорації, котра здійснює оперативно-дослідницькі навчання для моделювання різних форм щодо інформаційних атак в процесі інформаційної війни [17].

Метод дихотомії – це той метод, який може протистояти загрозам інформаційній безпеки, і необхідно вживати певні заходи на джерело загрози та на підсилення об’єкту захисту. Виокремлюються предметні області протидії (сукупність джерел загроз та сукупність заходів із забезпечення інформаційної безпеки) [17].

Методи впливу на інформацію у формі повідомлень представляються у вигляді [17]:

- Електронні методи – повідомлення фіксуються на електромагнітних носіях, які назначені на обробку завдяки засобів обчислювальної техніки. Їх мета знайти повідомлення на пристроях, які підлягають знищенню, модифікації та копіюванню повідомлень. Дані події реалізовані завдяки технічного та програмного забезпечення.
- Неелектронні методи – будуються на тій самій основі, але без

застосування засобів обчислювальної техніки для впливу на повідомлення (в такому випадку це паперові носії інформації).

Методи впливу на інформаційну інфраструктуру поділяються на [17]:

- Інформаційні методи направлені на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, та систем автоматизованої обробки інформації.
- Неінформаційні.

Вибір мети та методів протидії певним загрозам та небезпекам інформаційній безпеці являють собою складною проблематикою.

1.2 Основні види мережевих та комп'ютерних загроз в корпоративних мережах

Інформація вважається щось цінним та вимагає необхідного захисту, і варто розуміти, що захист інформації, ті ресурси, які виділяються на її захист має дорівнювати ціні самої інформації, але не перевищувати, так як у такому випадку, її оцінка перевищується, і немає бути навпаки, недооцінювати інформацію, економлячи на її захисті [29].

Основні шляхи несанкціонованого мережевого доступу до корпоративної інформації подано на Рис.1.1 [28,29].

Інформація має бути доступною для тих осіб, для яких вона має бути доступна, тобто розмежування доступу до інформації за ролями, і це наштовхує на створення комплексної системи інформаційної безпеки. Дана система повинна враховувати можливі джерела загроз (людський, технічний і стихійний чинники) та включати і собі комплекс захисних заходів: фізичних, адміністративних і програмно-технічних засобів захисту [29].

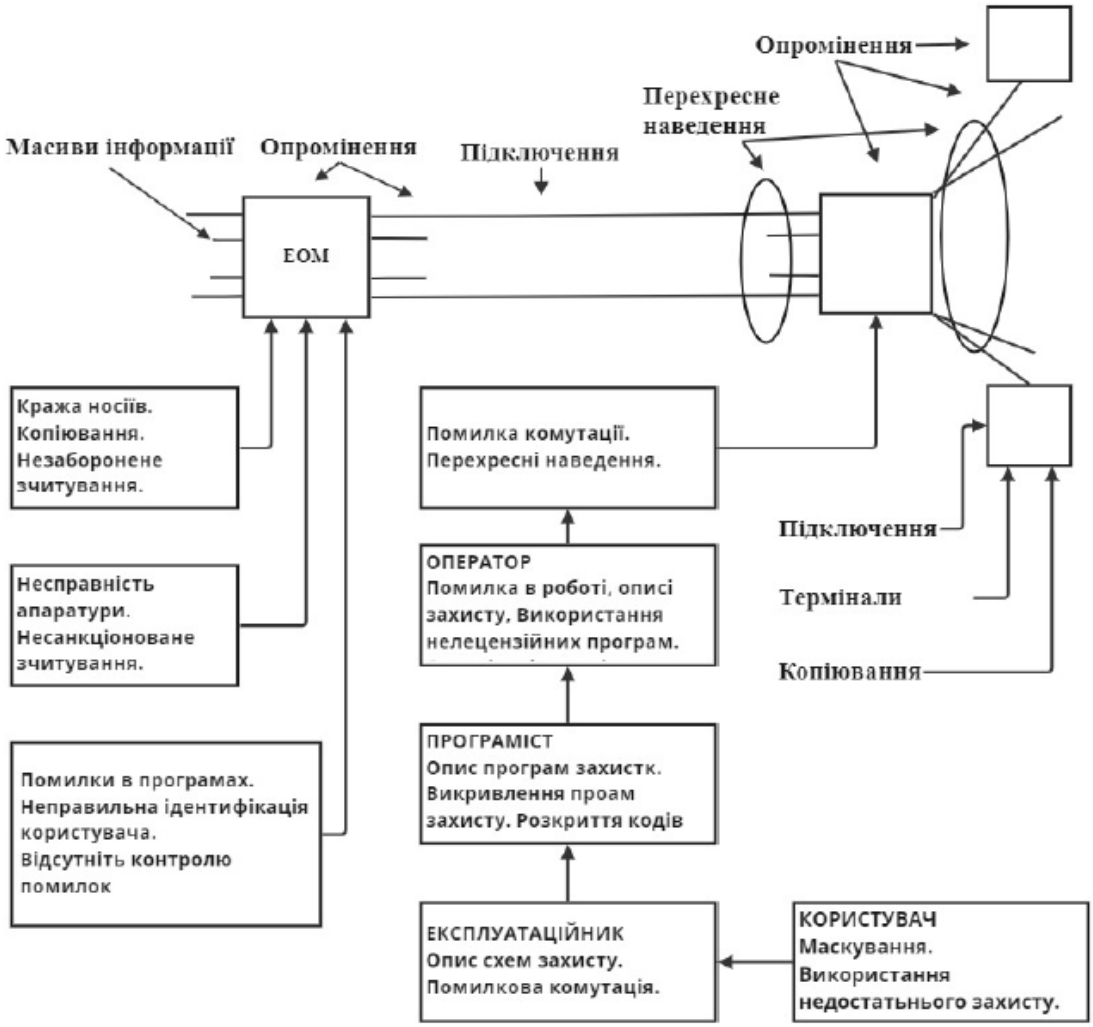

Рис.1.1 Основні шляхи несанкціонованого мережевого доступу до корпоративної інформації

Джерела загроз, які впливають на інформацію [29]:

1. Людський чинник – група загроз, яка залежить від дій людини, яка наділена роллю для доступу до інформації. І в свою чергу, джерело загрози поділяється на:

- зовнішні – дії осіб, які не наділені роллю для доступу до конкретної інформації, це можуть бути: кіберзлочинці, хакери, інтернет-шахраї, недобросовісні партнери, кримінальні структури;
- внутрішні – дії осіб, які наділені роллю для доступу до конкретної інформації, це можуть бути: персонал компанії та користувачі з домашніх комп’ютерів. Дії таких осіб можуть бути як умисними, так і неумисними.

2. Технічний чинник – група загроз, яка залежить та взаємопов'язана з технічними проблемами, наприклад, фізичне та моральне старіння апаратне забезпечення, неякісне чи не ліцензоване програмне та апаратне забезпечення. Як результат, це втрата інформації.

3. Стихійний чинник – це група загроз, яка залежить від природи, стихійних лих та інші можливі форс-мажорні обставини, і ця група загроз не залежить від людини.

Джерелами загроз не треба нехтувати при розробці системи чи підтримці існуючої. Слід звернути увагу на зовнішні загрози, так як ними найбільше нехтують [14]:

- Мережа Інтернет є глобальною та безмежною. Це надає можливість їй для розширення, розвитку веб-ресурсів та обміну інформацією. Тобто, будь-яка людина, котра має доступ до мережі Інтернет може отримати доступ до будь-якої інформації, яка є доступною для всіх чи створити власний ресурс. При цьому, розуміючи це, зловмисники та кіберзлочинці, намагаються використовуючи мережу для скоєння злочинів, де досить складно потім значти його місцезнаходження для покарання. Зловмисники розміщують віруси, шкідливі програми, «маскують» їх у програмному забезпеченні.
- Скрипти – це певний об'єкт, який запускається при відкритті веб-сторінки, та здійснює шкідливі дії на комп'ютері (зміна системного реєстру, крадіжка особистих даних, встановлення шкідливого програмного забезпечення, та інше). Застосовуючи мережеві технології, кіберзлочинці реалізують атаки на віддалені комп'ютери та сервери. Як результат, атаки виводять ресурс з ладу, тобто, інформація, котра зберігається на ньому. Як приклад, поява кредитних карт, електронних грошей, онлайн-банкінгів, то кількість інтернет-шахрайств зросло.
- Інтранет – це внутрішня мережа, яка розробляється для керування інформацією всередині компанії чи приватної домашньої мережі. Інтранет – простір для збереження, обміну та доступу до інформації для всіх комп'ютерів у конкретній мережі. І це може призвести до того, якщо хоча б один пристрій буде

заражено, то решта буде під загрозою. Для уникнення появи подібних ситуацій, варто забезпечувати захист не лише для конкретного периметру, але й для кожного комп'ютеру окремо.

- Електронна пошта – це застосунок, який є невід'ємною частиною нашої роботи, і в кожного працівника є обов'язкового особиста робоча електронна адреса, тому поштове програмне застосування у поєднанні з використанням шкідливих програм є ідеальною комбінацією для появи нових жертв кіберзлочинців. Користувач може навіть не підозрювати про проблему, яку він несе, тобто розсилка «заражених» листів своїм адресатам, і вже ті особи стають новими членами для розсилки «заражених» листів. Є навіть випадки, коли серйозні великі компанії потрапляли у ситуацію, де вони виступали відправниками «заражених» листів, і тоді страждають всі їх користувачі та персонал.
- Спам – небажана кореспонденція збільшує навантаження на поштові сервери, створюючи таким чином додатковий трафік та засмічує електронну пошту користувача, і може призвести до витрат робочого часу на їх видалення, що напряму пов'язано з фінансовими втратами. Кіберзлочинці застосовують технології для спаму масового розповсюдження з пропозицією перейти користувачу за посиланням, можливо, назва ресурсу буде подібною до того, яким він дійсно користується. Тому, задля забезпечення, варто фільтрувати листи та не відкривати взагалі від незнайомих адрес.
- Знімні носії інформації (CD/DVD-диски, флеш-карти, карти пам'яті та інше) не досить широко застосовується на сьогодні, так як на зміну прийшла «хмара», але все ж таки їх використовують для збереження та поширення інформації. Якщо активувати файл зі знімного носія, який містить у собі шкідливий код, то є загроза для пошкодження дані на комп'ютері чи розповсюдження вірусу на інші носії інформації чи мережі.

Види загроз, які виділяються спеціалістами з інформаційної безпеки [14]:

- Черви (Worms) застосовуються для розповсюдження недоліків операційної системи. Тобто, вони можуть завдяки мережі переходити з

комп’ютера на комп’ютер та впливати на електронну пошту та інші інформаційні канали. Їх особливість у тому, що їх швидкість досить висока У випадку проникнення, мають здатність обчислити мережеві адреси інших комп’ютерів та розіслати на адреси копії. Окрім мережевих адрес можуть бути використані дані з адресної книги поштових клієнтів. В такому випадку, представники цього класу шкідливих програм можуть створити робочі файли на дисках системи чи навіть не звертатися до ресурсів комп’ютера.

- Віруси (Viruses) – можуть завдати шкоди будь-яким програмам, додаючи в них власний код для отримання управління при запуску зараженого файлу.
- Троянські програми (Trojans) – мають властивість вражати комп’ютери: знищуючи інформацію на дисках, вплинути на швидкість роботи комп’ютеру – спричинити «зависання», крадіжка конфіденційної інформацію, та інше. Відрізняються від вірусів тим, що не впливають на роботу іншого програмного забезпечення. Не можуть самостійно потрапити на комп’ютер, і шкода від троянської програми може завдати більшої втрати від традиційної вірусної атаки.
- Програми-реклами (Adware) – певний програмний код, який включений у програмне забезпечення задля демонстрації реклами, не запитуючи при цьому користувача. Такі програми-реклами найчастіше включені до безкоштовного програмного забезпечення, так як розробникам необхідно отримувати кошти і від безкоштовного програмного забезпечення. Реклама розміщується на сторінках програми. Дані програми можуть загрожувати для користувача тим, що передають персональну інформацію, модифікація параметрів браузера та їх налаштування, створення неконтрольованого користувачем трафік.
- Програми-шпигуни (Spyware) – здійснюють збір інформації про конкретного користувача чи об’єкта інформаційної діяльності зокрема, не повідомляючи їх про це. Наявність таких програм-шпигунів може бути розміщена так, що користувач може навіть про це і не знати. Задачею таких

програм є [14]:

- відстеження дій користувача на комп’ютері;
- отримання інформації про зміст жорсткого диска;
- отримання інформації про якість зв’язку, спосіб підключення, швидкість модему тощо.
- Потенційно небезпечні додатки (Riskware) – програмне забезпечення, яке не є основним, а використовується додатково, і саме вони можуть містити у собі поломки й помилки, які можуть негативно вплинути на роботу системи в цілому. Такі програми можуть ваші дані піддати ризику. Такими програмами можуть виступати [14]:
  - Утиліти віддаленого адміністрування;
  - Програми автоматичної зміни розкладки клавіатури;
  - IRC-клієнти;
  - FTP-сервери;
  - Будь-які утиліти для зупинки процесів чи приховання їх роботи.
- Програми, котрі є вбудованими у браузер та впливають на перенаправлення трафіку. Тобто, при переході на один веб-сайт, відкривається інший.
- Програми-жарти (Jokes) – програми, які не впливають негативно на комп’ютер, але виводять повідомлення про існуючі проблеми чи можливі проблеми. Наприклад, про можливе форматування диску, виявлення вірусів чи інше.
- Програми-маскувальники (Rootkit) – програмне забезпечення, яке приховує шкідливу активність, тобто приховуються від виявлення їх антивірусними програмами. Такі програми, можуть модифікувати операційну систему чи вплинути на її функції, задля приховання своєї присутності, які завдає зловмисник на зараженому комп’ютері.
- Інші небезпечні програми – програмне забезпечення, яке направлене створення для організації DOS-атак на віддалені сервери, злому інших комп’ютерів, чи середовища розробки шкідливого програмного забезпечення.

Наприклад, така програма – Hack Tools.

Якщо звернути увагу на статистику, то найпоширенішими типами шкідливих програм є черви. Наступними у рейтингу віруси та троянські програми. Можуть бути навіть випадки, які поєднують у собі кілька наведених вище типів [14].

Класифікація комп'ютерний вірусів [4]:

- За об'єктами зараження.
- За способом зараження.
- За зовнішнім виглядом.
- За результатами діяльності.
- За кількістю засобів знешкодження.
- За способом створення вірусів.

Розглянемо детальніше кожен з цих способів окремо.

За об'єктами зараження [4]:

- файлові – вражають програмне забезпечення;
- завантажувальні – вражають завантажувальні сектори дисків;
- віруси структури файлової системи – модифікують в службові структури файлової системи.

Зміни відбуваються таким чином, де перший кластер програми є кластер, який містить код вірусу. І в процесу завантаження одразу спрацьовує вірус. Перший вірус – на основі даної технології DIR-вірус.

Приклади вірусів [4]:

- файлово-бутові,
- пакетні,
- мережеві,
- WinWord-віруси,
- Windows-віруси,
- OS/2-віруси,
- Novell NetWare-віруси,
- BIOS-віруси,

- CD-ROM-віруси тощо.

За способом зараження місцезнаходження вірусів [4]:

- Резидентні.
- Нерезидентні.

За зовнішнім виглядом [4]:

- звичайні – код вірусу одразу можна визначити на диску;
- невидимі (Stealth-віруси) – застосовують особливі методи маскування, де при перегляді диску одразу код вірусу не видно. Такі віруси мають резидентний модуль, який знаходиться в оперативній пам’яті комп’ютеру. Маскування здійснюється, якщо на запам’ятовуючому пристрої знаходиться резидентний модуль вірусу. Якщо операційну систему (ОС) завантажувати з дискети, вірус не матиме змогу отримати керування ПК та механізм не спрацює;
- поліморфні – код вірусу змінний.

За результатами діяльності [4]:

- безпечні – поширюють себе таким чином, щоб проявляти себе у вигляді повідомлень, перезавантаження та інших несподіваних не зовсім зрозумілих ефектів, але без втрати інформації чи шкоди апаратному забезпеченню та програмному забезпеченню;
- небезпечні – навпаки, призводять до втрати інформації, руйнуванню обчислювальної системи, тобто програмного та апаратного забезпечення.

За кількістю засобів знешкодження, де можуть бути знешкоджені [4]:

- однією антивірусною програмою (AVO-віруси).
- кількома антивірусними програмами (комплектом N антивірусів – AVN-віруси).

За способом створення вірусів, де можуть бути створені [4]:

- ручними засобами розробки (H-віруси).
- автоматизованими засобами розробки (A-віруси).

1.3 Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність

Протокол мережевої безпеки IPSec Internet Protocol Security (IPSec) – це погоджений набір відкритих стандартів, який наразі має конкретну специфікацію, та доповнюється новими протоколами, алгоритмами та функціями мережевої безпеки [19].

Головне призначення протоколів IPSec – є забезпечення безпечної передачі даних IP-мережами, а їх використання забезпечує [19]:

- цілісність – здатність мережі забезпечувати передачу даних без модифікації, втрати чи дублювання;
- автентичність – здатність мережі забезпечувати передачу даних задля можливості підтвердити чинність, які саме дані передаються відправником, та за кого він себе видає;
- конфіденційність – здатність мережі забезпечувати передачу даних у формі, котра запобігає їх несанкціонованому перегляду.

Специфікація IPSec розробляється робочою групою IP Security Protocol IETF, дана специфікація включає у собі 3 алгоритмо-незалежні базові специфікації, і саме вони публікуються як RFC-документ «Архітектура безпеки IP» – RFC1825, «Автентифікований заголовок» – RFC1826, «Інкапсуляція зашифрованих даних» – RFC1827 [19].

У листопаді 1998 року робоча група IP Security Protocol IETF, пропонується нова версія даних документів – це RFC2401 – RFC2412. Версії такі як RFC1825-27 не застосовуються, так як є застарілими [9].

Робоча група IP Security Protocol займається розробкою та протоколами управління ключовою інформацією. Задачею якої є розробка Internet Security Association and Key Management Protocol (ISAKMP) – протокол керування ключами прикладного рівня, не залежного від застосованих протоколів забезпечення безпеки [9].

Основними компонентами IPsec вважаються [9]:

- RFC2402 «IP Authentication Heade» (AH) – застосовується для

цілісності та автентичності пакетів даних в IP-мережі;

- RFC2406 «IP Encapsulation Security Payload» (ESP) – застосовується для забезпечення конфіденційності, цілісності та автентичності пакетів даних у IP-мережі;
- RFC2408 «ISAKMP» – застосовується для забезпечення погодження параметрів, формування, модифікації, видалення контекстів із захищених з'єднань (Security Association, SA) та керування ключами в IP-мережах;
- RFC2409 «The Internet Key Exchange» (IKE) – подальший розвиток та адаптацією ISAKMP, котра використовується для роботи за протоколами IPSec.

Ядро IPSec формується на трьох протоколах [9]:

- протокол автентичності (AH).
- протокол шифрування (ESP).
- протокол обміну ключами (IKE).

Функції задля підтримки захищеного каналу поділяються між вказаними протоколами наступним чином [36]:

- протокол AH забезпечує цілісність та автентичність даних;
- протокол ESP зашифровує дані, які передаються, гарантуючи конфіденційність, можлива підтримка автентифікації та цілісності даних;
- протокол IKE вирішує допоміжну задачу автоматичного надання секретних ключів, які необхідні для роботи протоколів автентифікації та шифрування даних.

Можливість протоколів AH та ESP частково перекриваються. Де, перший протокол відповідає лише за контроль цілісності та автентифікацію даних, тоді, як протокол ESP дозволяє зашифрувати дані та здійснити функції першого протоколу. Задля забезпечення цілісності та автентифікації пакетів даних застосовуються спеціальні механізми за контролем цілісності та автентичності, котрі базуються на присвоєнні, котрі передаються [36].

Задля забезпечення ефективного функціонування протоколів застосовується інший протокол IKE, котрий встановлює між цими двома точками логічне з'єднання [36].

Встановлення SA розпочинається за взаємної автентифікації. Параметри SA визначаються, який саме з двох протоколів використовується для захисту даних. Прикладом може бути, здійснюється лише автентифікація та перевірка цілісності чи захист від помилкового відтворення. Протоколи AH та ESP здійснюють захист даних у двох режимах: транспортний та тунельний [36].

Транспортний режим – це передача IP-пакету здійснюється завдяки оригінального заголовка даного пакету даних. Перевага транспортного режиму полягає у зменшенні обчислювальних та комунікаційних витрат [36].

Тоді як, забезпечення безпеки телекомунікаційної мережі задля транспортного режиму з функціонування протоколів AH та ESP, якому належать наступні недоліки [36]:

- ESP не здатен захистити заголовок пакету даних;
- Неможливо приховати топологію мережі, так як заголовок пакетів передаються у відкритому вигляді.

Тунельний режим – режим, де вихідний IP-пакет може розміститися у новому, далі реалізується передача даних мережею, котра ґрунтується на підставі заголовка нового IP-пакету [11].

Режим ґарантує захист заголовку пакету даних, де як результат приховується топологія мережі – це є безумовною перевагою при побудові захищених систем і мереж. Реалізація тунельного режиму потребує великих обчислювальних та комунікаційних ресурсів [11].

Застосування будь-якого з цих режимів залежать від вимог, які необхідні для захисту даних та ролі, які мають досягатися у мережі та завершальний канал. Вузол може бути хостом або шлюзом [11].

Протокол ESP використовується в тунельному та в транспортному режимі, окремо чи у поднанні з протоколом AH [11].

Транспортний режим застосовується для захисту поля даних IP пакета, який містить протоколи транспортного рівня (TCP, UDP, ICMP) та включає у собі інформацію прикладних служб [23].

Використання транспортного режиму – це передача електронної пошти. Проміжними вузлами на маршруті пакету застосовують лише відкриту інформацію мережевого рівня. Недолік транспортного режиму – це відсутність механізмів приховання даних відправника та одержувача пакету та можливість аналізу трафіку. Результат даного аналізу – є отримання інформації щодо об'єму та напрямів щодо передачі інформації та інше [23].

Тунельний режим передбачає захист та шифрування пакету, які включають заголовок мережевого рівня. Тунельний режим використовується у випадку приховання інформаційного обміну організації з зовнішнім світом [23].

Адресні поля заголовку мережевого рівня пакету, який застосовується тунельний режим, який заповнюються міжмережевим екраном організації та не містить інформацію щодо конкретного відправника пакету. У випадку передачі інформації ззовні в локальну мережу організації, наприклад, адреса призначення, то застосовується мережева адреса міжмережевого екрану. Після здійснення розшифрування міжмережевим екраном, то заголовок мережевого рівня направляється одержувачу [23].

Протокол Secure Socket Layer (SSL) розробляється для забезпечення надійного захисту наскрізної передачі даних із застосуванням TCP. Протокол SSL становить не один протокол, а складається з двох рівних протоколів [33].

Протокол SSL – базовий набір засобів захисту інформації, котрий використовується протоколами на більш високих рівнях та забезпечує конфіденційність каналу комунікацій та автентифікацію користувача [33].

Протокол діалогу SSL має дві основні фази [33]:

- Перша фаза – застосовується для встановлення конфіденційного каналу комунікацій.
- Друга – застосовується для автентифікації користувача.

Протокол TLS застосовується для забезпечення конфіденційності та цілісності даних [33].

Складається з двох рівнів [33]:

- протокол записів TLS;

- протокол діалогу TLS.

Протокол записів TLS забезпечує конфіденційність даних із застосуванням симетричних алгоритмів шифрування: DES, RC4 та цілісність даних з використанням гешфункцій SHA-1 чи MD5 [2].

Протокол діалогу TLS забезпечує кваліфікований електронний підпис, який ґрунтується на RSA чи DSS [2].

Висновки по розділу 1

У першому розділі кваліфікаційної роботи розглянуто аналіз порушень інформаційної безпеки, де визначено рівні інформаційної безпеки, характеристики інформаційної безпеки, типи методів для забезпечення інформаційної безпеки на об’єкті інформаційної діяльності ,методи впливу на інформацію у формі повідомлень.

Проаналізовано основні види мережевих і комп’ютерних загроз, джерела загроз, які впливають на інформацію та протоколи захисту та цілісності IPSec, SSL, TLS.

Розділ 2 КЛАСИФІКАЦІЯ ЗАГРОЗ ТА АТАК НА КОРПОРАТИВНІ МЕРЕЖІ

2.1 Класифікація загроз інформації в комп'ютерній системі

Поняття «загрози для безпеки інформації» – це певна дія, яка направлена проти об'єкта захисту, який проявляється в небезпеці модифікацій та втрат інформації. Джерелами загроз для безпеки інформації можуть виступати як зовнішні, так і внутрішні загрози [2].

Згідно аналізу, джерела загроз, які можуть виникнути для безпеки інформації, котра циркулює у корпоративній мережі, то вони поділяються на кілька груп [2]:

- Загрози антропогенні;
- Загрози техногенні;
- Загрози природні загрози.

Перша група є найбільшою та найбільш привабливою до обговорень, так як дії суб'єкта завжди можна зараніше оцінити, спрогнозувати та вжити превентивних заходів [2].

Суб'єкти, дії котрих призводять до порушення інформаційної безпеки [2]:

- Зовнішні (конкуренти, невідповідальних партнерів, політичних супротивників);
- Внутрішні (співробітники організації).

У залежності від того, чи належить джерело загрози до однієї з категорій, антропогенної, техногенної або природньої категорії [1].

До першої категорії (антропогенної) включаємо загрози, які обумовлені діями суб'єктів та призводять до низки небажаних наслідків, серед них можемо виділити [1]:

1. Крадіжка:

а) технічних засобів (вінчестерів, ноутбуків, системних блоків);

б) носіїв інформації (паперових, магнітних, оптичних та ін.);

в) інформації (читання й несанкціоноване копіювання);

г) засобів доступу (ключі, паролі, ключова документація та ін.).

2. Підміна (модифікація):

а) операційних систем;

б) систем керування базами даних, прикладних програм;

в) інформації (даних);

г) заперечення факту відправлення повідомлень;

д) паролів і правил доступу.

3. Знищення (руйнування):

а) технічних засобів (вінчестерів, ноутбуків, системних блоків);

б) носіїв інформації (паперових, магнітних, оптичних та ін.);

в) програмного забезпечення (ОС, СУБД, прикладного ПЗ);

г) інформації (файлів, даних);

д) паролів і ключової інформації.

4. Порушення нормальної роботи (переривання):

а) швидкості обробки інформації;

б) пропускної здатності каналів зв’язки;

в) обсягів вільної оперативної пам’яті;

г) обсягів вільного дискового простору;

д) електроживлення технічних засобів.

5. Помилки:

а) при інсталяції ПЗ, ОС, СУБД;

б) при написанні прикладного ПЗ;

в) при експлуатації ПЗ;

г) при експлуатації технічних засобів.

6. Перехоплення інформації:

а) за рахунок ПЕМВ від технічних засобів;

б) за рахунок наведень по лініях електроживлення;

в) за рахунок наведень по сторонніх провідниках;

г) по акустичному каналу від засобів виводу;

д) по акустичному каналу під час обговорення питань;

е) при підключенні до каналів передачі інформації;

ж) за рахунок порушення встановлених правил доступу (злом).

Друга категорія (техногенні) містить загрози, які залежать від технічного обладнання. Технічні засоби можуть містити у собі потенційні загрози безпеки інформації, і при цьому можуть бути [27]:

- Внутрішніми:

- неякісні технічні засоби обробки інформації;

- неякісні програмні засоби обробки інформації;

- допоміжні засоби (охорони, сигналізації, телефонії);

- інші технічні засоби, застосовувані в установі;

- Зовнішніми:

- засоби зв’язку;

- близько розташовані небезпечні виробництва;

- мережі інженерних комунікації (енерго- і водопостачання, каналізації);

- транспорт.

Наслідками застосування даних технічних засобів, які впливають на безпеку інформації можуть бути [27]:

1. Порушення нормальної роботи:

а) порушення працездатності системи обробки інформації;

б) порушення працездатності зв’язку й телекомунікацій;

в) старіння носіїв інформації й засобів її обробки;

г) порушення встановлених правил доступу;

д) електромагнітний вплив на технічні засоби.

2. Знищення (руйнування):

а) програмного забезпечення, ОС, СУБД;

б) засобів обробки інформації (кидки напруг, протічки);

в) приміщень;

г) інформації (розмагнічування, радіація та ін.);

д) персоналу.

3. Модифікація (зміна):

а) програмного забезпечення. ОС, СУБД;

б) інформації при передачі по каналах зв’язку й телекомунікаціям.

Третю групу становлять загрози (природні), котрі спрогнозувати неможливо. Так як стихійні джерела, які становлять потенційні загрози інформаційної безпеки є зовнішніми, то варто розглянути природні катаклізми [27]:

- пожежі;
- землетруси;
- повені;
- урагани;
- інші форс-мажорні обставини.

Такі явища впливають на інформаційну безпеку, небезпечні елементи корпоративної мережі призводять до наступних наслідків [27]:

1. Знищення (руйнування):

а) технічних засобів обробки інформації;

б) носіїв інформації;

в) програмного забезпечення (ОС, СУБД, прикладного ПЗ);

г) інформації (файлів, даних);

д) приміщень;

е) персоналу.

2. Зникнення (викрадення):

а) інформації в засобах обробки;

б) інформації при передачі по телекомунікаційних каналах;

в) носіїв інформації;

г) персоналу.

Як результат, відповідно до класифікації котра описана вище, варто зазначити, що її застосування у процесі підготовки та створення вихідних даних для побудови системи захисту інформації надає можливість привести до ладу роботу, уникнути зайвих витрат часу на збір даних, зменшити ймовірність

випадкових помилок та звернути увагу на вивчення та опис критичних загроз [27].

В цілому, класифікація надає можливість диференційовано розподілити ресурси, які виділяються на забезпечення інформаційної безпеки [27].

2.2 Класифікація мережевих атак та методи протидії і захисту

В умовах сучасності, розвиток інформаційного середовища найбільшого поширення зазнає ІТ-технології. Комп'ютерні мережі є напрямок, основним ресурсом виступає інформація [18].

Одночасно з розвитком технологій передачі даних, розвиваються навички кіберзлочинців, які активно атакують комп'ютерні мережі [18].

Типи мережевих атак є [18]:

1. Сніффер пакетів – прикладна програма, котра застосовує мережеву карту, котра працює в некоректному режимі. Перехоплення IP-пакетів, які передаються через конкретний сегмент.

Задля зменшення наслідків від сніффінга пакетів, то можна застосовувати наступні засоби:

- Автентифікація – завдяки сильним засобам автентифікації застосовується спосіб – одноразові паролі (OTP – OneTime Passwords). Тобто, OTP – це певна технологія двофакторної автентифікації, де поєднується, те що у вас вже є з тим, що ви знаєте. Наприклад, двофакторна автентифікації – банкомат, де використовується Ваша карта та Ваш пін-код до неї.
- Комутована інфраструктура – завдяки комутованій інфраструктурі здійснюється боротьба зі сніффінгом пакетів у мережеві. Прикладом може бути, застосуючи комутований Ethernet, зловмисники отримавши доступ лише до трафіку, який знадходить той же порт, до якого було здійснено підключення.
- Анти-сніфери – завдяки встановленні апаратного та програмного забезпечення, здійснюється боротьба з анти-сніферам, таким чином можна розпізнати сніфери, які існують у комп'ютерній мережі. Засоби не дозволяють

повністю вирішити загрозу, власне як і інші засоби поодиночку.

- Криптографія – найефективнішим способом на сьогодні вважається криптографія, таким чином зводячи на нівець роботу сніфферів.

2. IP-спуфінг здійснюється, тоді коли хакер, який знаходиться в корпорації чи поза нею, показує себе (представляє себе), як чинного користувача. Реалізація можлива двома способами. Перший – застосування IP-адрес, який знаходиться в межах діапазону дозволених IP-адрес, другий – наданий дозвіл для конкретної зовнішньої адреси, які надано дозвіл до конкретних мережевих ресурсів.

Загроза спуфінга частково вирішується, але не ліквідувати завдяки:

- Контроль доступу – один з найпростіших спосіб для запобігання IP-спуфінга. Дозволяє обрати найпідходящий метод для управління доступом. Для зниження ефективності IP-спуфінга, тому слід відхилити сторонній трафік, який надходить із зовнішньої мережі.
- Фільтрація за RFC 2827. Для припинення спроб спуфінга від чужих мереж, користувачами Вашої мережі. Блокуючи будь-який вихідний трафік, адреса джерела, котра не належить до IP-адрес Вашої організації.
- Автентифікація можлива, якщо здійснюється на базі IP-адрес. Для інтеграції додаткових методів автентифікації здійснює даний вид атак неліквідним.

3. Парольні атаки, здійснюються, завдяки певної кількості методів, якими можуть виступати: простий перебір, «троянський кінь», IP-спуфінг та сніффінг пакетів.

Задля уникнення парольних атак необхідно здійснити інший підхід до вибору паролю, тобто, не слід використовувати паролі в текстовій формі. Одноразові паролі та/чи криптографічна автентифікація зводить нанівець такі атаки.

Адміністратори для боротьби з такими атаками використовують кілька методів: використання засобу L0phtCrack, який найчастіше використовується зловмисниками для підбору паролів у середовищі Windows NT. За допомогою,

даного засобу можна визначити, як просто підібрати пароль, який обрано користувачем для автентифікації.

4. Атаки на рівні застосунків можуть бути здійснені кількома способами.

Серед них найрозповсюдженішими є використання вразливих місць серверного програмного забезпечення (наприклад, sendmail, HTTP та FTP). Зловмисники, отримавши доступ до комп'ютера від імені користувача, який працює з застосуванням. Відомостями щодо атак на рівні застосування широко публікуються, задля можливості адміністраторам виправити проблему завдяки корекційних модулів (патчі). Але, зловмисники аналогічним чином, зможуть отримати доступ до даних відомостей, що дозволяє їм практикуватися.

5. Мережева розвідка – збір певної інформації щодо мережі завдяки загальнодоступних даних та застосувань. У процесі атаки проти будь-якої мережі зловмисник намагається отримати максимальну кількість більше інформації. Мережева розвідка здійснюється у формі запитів DNS, ехо-тестування та сканування портів. Запити DNS надають можливість володіти доменом та адреси домену привласнені. Ехо-тестування адрес, розкриваються завдяки DNS, дозволяють проаналізувати хости, які дійсно працюють у даному середовищі.

Отримавши список хостів, зловмисниками використовуються засобами сканування портів для складення списку послуг, які надаються даними хостами. Зловмисник, аналізуючи характеристики застосувань, які працюють на хостах. Як результат, отримується інформація, яка використовується для злому.

Повністю вирішити питання, від атаки – мережевої розвідки неможливо.

6. Соціальна інженерія – досить простий та легкий способів злому, який ґрунтується на роботі зі співробітниками компанії, вплив на них чи обман. Прикладом може бути, тоді як зловмисник вводячи в оману співробітника організації, представляючи себе як мережевого адміністратора, для отримання паролю.

Протидією даного методу є проводження навчання, підготовку співробітників та фіксація даних навчань та вимог у політиці безпеки правил поведінки співробітника організації.

Це лише є короткий список мережевих атак, які серйозно закріпилися серед загроз, тому варто приділити увагу мережевикам та безпековцям для запобігання можливих атак. Аналітику безпеки та системному адміністратору, варто розуміти підходи для вирішення таких проблем.

2.3 Безпека корпоративних мереж та основні мережеві атаки на них

Безпека комп'ютерної системи – процес забезпечення конфіденційності та цілісності. І система може вважатися безпечною, за умови використання ресурсів та отримання доступу за призначенням за будь-яких обставин, але ні одна система не зможе гарантувати абсолютну безпеку від кількох різних шкідливих загроз та несанкціонованого доступу [35].

Безпека системи загрожує лише через два порушення [35]:

– Загроза: програма, котра завдає серйозні шкоди системі.

– Атака: спроба зламати безпеку та несанкціоновано використовувати актив.

Порушення безпеки, котра впливає на систему класифікується за типами: зловмисні та випадкові [35].

Зловмисні загрози – шкідливий комп'ютерний код, який розробляється для створення вразливості системи, котра призводить до порушень безпеки. Але, з іншого боку, від випадкової загрози порівняно простіше захиститися [35].

Безпека порушується через будь-яке зі згаданих порушень [35]:

1. Порушення конфіденційності – порушення, які передбачають несанкціонований доступ до даних.

2. Порушення доступності – несанкціоноване знищення даних чи несанкціоновану модифікацію даних.

3. Крадіжка служби – несанкціоноване застосування ресурсів.

4. Відмова в обслуговуванні – недопущення законного використання системи.

Напади мають абсолютно випадковий характер.

Основна мета інформаційної безпеки є гарантування [15]:

- Цілісність. Тобто, до об’єктів у системі має бути доступ до санкціонованого користувача, а користувач, який не наділений відповідними правами, то не повинен мати можливості змінювати системні файли та ресурси. Системні об’єкти мають бути доступними лише певним авторизованим користувачам, тобто не всі мають можливість переглядати системні файли.
- Наявність. Тобто, системні ресурси мають бути доступними лише авторизованим користувачам, варто зауважити, що наділений правами не тільки один користувач до системних ресурсів. Тоді, зловмисне програмне забезпечення може приєднати ресурси до себе, тобто не допускаючи до законних процесів доступу до системних ресурсів.

Широковикористовувана загроза – комп’ютерний хробак – є комп’ютерна програма, котра заражає комп’ютер через мережу. Відрізняється від звичайного вірусу, то вона активно працює над локальною мережею. Комп’ютер, який є заражений від хробака, то він атакує цільову систему та записує на неї невелику програму – «гачок», котра застосовується для копіювання хробака на цільовий комп’ютер. Даний процес є рекурсивним таким чином, процес зчеплює всі системи локальної мережі, вона застосовує механізм нересту для дублювання себе ж. Хробак копіює сам себе, на основі застосування більшості системних ресурсів та блокуючи всі інші процеси [15].

Ключова функціональність хробака має представлятися як сканування портів – це засіб, завдяки якого зловмисник визначає вразливість системи для реалізації атаки – вважається автоматизованим процесом, котрий включається у формування TCP/IP-з’єднання до певного порту [15].

Для захисту особи зловмисника, атака сканування портів здійснюється від Zombie Systems, мається на увазі, систем, котрі раніше вважалися незалежними системами, котрі обслуговують своїх власників. Дані атаки не направлені на збір інформації чи знищення системних файлів. Скоріше за все, застосовуються для порушення законного застосування інформаційної системи. Дані атаки використовуються на комп’ютерні мережі [15].

Такі атаки поділяються на дві категорії [13]:

– Перша категорія застосовує таку кількість системних ресурсів, що подальша робота не є можливою. Прикладом може бути, скачування файлу з веб-сайту, який навантажує весь доступний ресурс процесора;

– Друга категорія використовує зрив мережі об’єкта. Дані атаки є наслідком зловживання певними основними принципами функціональних можливостей TCP/IP.

Для реалізації захисту комп’ютерної системи заходи безпеки застосовуються на наступних рівнях [13]:

- Фізичний рівень – об’єкти, котрі входять у комп’ютерні системи, та повинні бути фізично захищені від кіберзлочинців. Робочі станції мають ретельно захищатися, і лише відповідні користувачі мати дозвіл на доступ до системи. Варто запобігати фішингу та дайвінгу.
- Рівень операційної системи – система має захистити себе самостійно від випадкових чи цілеспрямованих порушень безпеки.
- Мережевий рівень – поділ інформації між різними системами через мережу. Перехоплення даних у такому випадку може бути шкідливим, та можна його порівняти з вторгненням у комп’ютер. Тому приділяти захист і мережевому рівню варто. Як приклад, застосування програмного забезпечення Anti Malware достатньо для поверхневого виявлення та видалення вірусів та загроз. Вбудовані брандмауери також можуть справлятися с такими мережевими загрозами.

Висновки по розділу 2

У другому розділі кваліфікаційної роботи було класифіковано загрози інформації, мережеві атаки та запропоновано методи їх протидії, реалізація безпеки комп’ютерних систем.

Але варто розміти, що захист інформації не має обмежуватися технічними методами. Для ефективного забезпечення інформаційної безпеки варто поєднувати різні моделі та методи оцінки загроз та небезпек.

Інформація є ключовим надбанням та вимагає належного захисту. Тоді як інформація має бути доступною для певного кола користувачів. Тобто, постає питання щодо створення комплексної системи інформаційної безпеки в організації. Дана система має враховувати всі можливі джерела загрози, які були перераховані у розділі, застосовувати весь спектр захисних заходів: фізичних, адміністративних і програмно-технічних засобів захисту.

Окрім цього, розробляються апаратні пристрої для захист мереж на об’єкті інформаційної діяльності. Які успішно використовуються, але незмінними та традиційними залишаються – спеціальне програмне забезпечення.

У процесі вивчення проблем інформаційної безпеки важливо виділити загрози для інформаційної безпеки, аналіз захисту від таких загроз.

Загроза інформаційній безпеці – явище, події від негативних чинників чи процес, де соціальні об’єкти інформаційної безпеки частково чи повністю втрачають можливість реалізувати власні інтереси в інформаційній сфері; порушення стандартного функціонування, здійснення руйнування та стримання розвитку технічних об’єктів інформаційної безпеки.

Безпека комп’ютерних мереж – це досить складне питання для кожної організації, котра включає у собі великий перелік аспектів комп’ютерних технологій, мереж управління, застосування мережі та їх підтримка. Задля підвищення безпеки комп’ютерної мережі варто займатися розробкою ефективних рішень безпеки, заходи для покращення безпеки комп’ютерних мереж. Тому для проходження складного шляху, варто забезпечити нормальну роботу мережевої комп’ютерної системи для об’єкту інформаційної діяльності.

Розділ 3 МЕТОДИ ЗАХИСТУ ВІД КІБЕРАТАКИ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Технічні заходи у сфері забезпечення інформаційної безпеки в корпоративних мережах

Для реалізації ефективних заходів задля забезпечення захисту інформації необхідна не лише розробка засобів захисту інформації в мережі, але й розробка механізмів моделі захисту інформації та реалізація системного підходу чи комплексу із захисту інформації [30].

Комплекс захисту інформації базується на спеціальних технічних та програмних засобів для організації заходів із захисту інформації [30].

Розрізняються кілька ключових засобів захисту інформації [30]:

- Технічні;
- Програмні;
- Криптографічні;
- Організаційні; .

Наразі існує безліч технічних рішень для забезпечення інформаційної безпеки [30].

Такими технічними заходами є [30]:

- міжмережеві екрани (апаратне та програмне забезпечення);
- антивірусні програми;
- системи з запобігання витоків даних;
- системи з запобігання вторгнень;
- системи з резервного копіювання та відновлення інформації;
- системи з відеоспостереження;
- системи з контролю доступу в приміщення.

Дані технічні заходи відрізняються за ціною та функціями. Вибір конкретних рішень має ґрунтуватися на ризик-аналізі [30].

Проблемами інформаційної безпеки у сфері технічного захисту інформації [7]:

- Перехоплення електронного випромінювання – проблема, яка вирішується забезпеченням захисту інформації, котра передається радіоканалами зв’язку та обміну даними у інформаційній системі;
- Примусове електромагнітне опромінення ліній зв’язку для отримання паразитної модуляції – проблема, яка вирішується завдяки інженерного чи фізичного захисту інформації.

До них, можуть бути віднесені – захист інформації в локальних мережах, в інтернеті та інших технічних засобів інформаційної безпеки [7]:

- Застосування підслуховуючих пристроїв;
- Копіювання носіїв інформації з подоланням заходів захисту;
- Маскування під зареєстрованого користувача;
- Маскування під запити системи;
- Використання програмних пасток;
- Використання недоліків мов програмування і операційних систем;
- Незаконне підключення до апаратури та ліній зв’язку спеціально розроблених апаратних засобів, які забезпечують доступ до інформації;
- Зловмисне виведення з ладу механізмів захисту;
- Розшифрування спеціальними програмами зашифрованої інформації;
- Інформаційні інфекції.

Для запобігання вищевказаних каналів витоку інформації за оцінкою інформаційної безпеки, варто володіти необхідними знаннями та потрібною освітою, мати високий рівень знань при виборі та використанні та програмних засобів захисту інформації. Без комплексного підходу для захисту інформації з застосуванням описаних засобів вимагає дотримання політики безпеки на всіх рівнях діяльності підприємства [7].

3.2 Захист інформації на мережевому рівні

Для захисту мереж використовуються певні засоби захисту [10]:

- міжмережеві екрани – застосовуються для блокування атак, які надходять із зовнішнього середовища. Їх задача управляти проходженням мережевого трафіку відповідно до правил захисту.

Такі екрани розміщуються на вході мережі та поділяють на внутрішні (приватні) та зовнішні (загального доступу) мережі;

- системи виявлення втручань – застосовуються для виявлення спроб несанкціонованого доступу, які надходять ззовні та всередині мережі. Їх задача здійснювати захист від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми дані системи можуть попередити шкідливі дії, які дозволяють знизити час простою внаслідок атаки та витрати на підтримку працездатності мережі;

- засоби для формування віртуальних приватних мереж – застосовуються для організації захищених каналів передачі даних через незахищене середовище.

Такі мережі забезпечують прозоре для користувача поєднання локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації завдяки її динамічного шифрування;

- засоби аналізу захищеності – застосовуються для аналізу захищеності корпоративної мережі, виявлення потенційних каналів реалізації загроз інформації. Використання таких засобів надає можливість попередити потенційні атаки на корпоративну мережу, оптимізувавши витрати на захист інформації та контролювати поточний стан захищеності мережі.

3.3 Засоби і методи захисту від мережевих комп’ютерних загроз

Програмні засоби захисту інформації надають можливість ідентифікації та автентифікації користувачів, розмежовуючи доступ до ресурсів відповідно до ролей, які надані користувачам, та інше [21].

Програмні засоби захисту інформації будуються на стеганографічних методах. Де, «стеганографія» – приховане письмо, котре не дає можливості сторонній особі дізнатися про його існування. Згадка про використання тайнопису датується V століттям до н. е. А вже на сьогодні це роздрукування на ЕОМ контрактів з малопомітними викривленнями окремих символів тексту – таким чином, фіксувалася шифрована інформація про умови складання контракту [21].

Комп'ютерна стеганографія ґрунтується на двох принципах [21]:

- Аудіо- і відеофайли, оцифровані файли можна модифікувати навіть без втрати функціональності.
- Розпізнання людиною зміни кольору чи звуку обмежені.

Стеганографія частіше за все застосовується для створення цифрових водяних знаків, де від звичайних вони відрязняються тим, що вони наносяться спеціальним програмним забезпеченням (цифрові водяні знаки записуються у вигляді псевдовипадкових послідовностей шумових сигналів, які згенеровані на основі секретних ключів). Дані водяні знаки забезпечують автентичність чи недоторканість документу, ідентифікація автора чи власника, перевірка права власності, навіть за умови, що файл оброблений чи модифікований [21].

Для інтеграції засобів програмно-технічного захисту в мережі можливе у таких варіаціях [21]:

- Додатковий захист – засіб захисту вважається додатком до основного програмного та апаратного засобів комп'ютерної системи. Вважається досить гнучким та пристосованим, який можна додати як вручну такі і за необхідністю, у процесі можливі проблеми із сумісністю програмно-апаратного забезпечення, тому перед вибором варто звернути увагу на сумісність обох методів захисту.
- Вбудований захист – механізм захисту реалізується як окремий компонент цілої системи чи розподіляється за іншими компонентами системи.

Вмонтований захист є більш надійним та оптимальним, але досить складним з боку додавання чи внесення будь-яких змін. Перевагою є можлива комбінація з різними системами.

Для виявлення, знищення та попередження заражень мережі використовуються загальні засоби захисту інформації та профілактика, котрі зменшують ймовірність зараження. Останні роки розробляються апаратні пристрої антивірусного захисту, серед них досить поширеним методом залишається застосування антивірусних програм – спеціальні програми, котрі призначаються для виявлення та знищення комп'ютерних вірусів [21].

Антивірусні програми у свою чергу поділяють на [16]:

• Програми-детектори реалізують пошук сигнатур вірусів. Недолік – можуть реалізовувати пошук лише тих вірусів, які є відомі на даний момент, але при цьому база даних таких вірусів швидко старіє, і її необхідно постійно оновлювати. Програми-детектори не можуть наперед виявити невідомий вірус. Тобто, якщо не знайдено вірус, то не факт, що його дійсно немає. Детектори мають режими лікування чи знищення заражених файлів – функції докторів.

• Програми-лікарі реалізують пошук заражених файлів та намагаються їх очистити від вірусу, таким чином відновлюючи. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед програм-лікарів виокремлюють ті, котрі призначаються для пошуку та знищення великої кількості вірусів. Такі прогами потребують постійного оновлення.

• Програми-ревізори реалізують можливість запам'ятовувати початковий стан програм, каталогів та системних реєстрів, тоді як комп'ютер не заражається вірусом, але з часом (відповідно періоду чи за згодою користувача), порівнюється поточний стан системи з початковим. Перевірка реалізується одразу після завантаження операційної системи – контролюються довжина файлу, контрольна сума, дата та час модифікації, інша необхідна інформація. Такі програми можуть допомогти виявляти і стелс-віруси. Модифіковані програм та лікарів не виявляють зміни, але й повернути файли та системні області до початкового стану. Такі програми є універсальними у порівнянні з

вищеописаними, так як захищають від вірусу, який з’явиться у майбутньому.

- Програми-фільтри – програми, котрі призначені для знаходження підозрілих дій у процесі роботи комп’ютера. Після отримання повідомлення користувач або погоджується чи відкликає здійснення операції. Програми можуть здійснити перевірку програми, котрі викликаються до виконання та ті файли, які копіюються. Недоліки – настирність, конфлікти з іншим програмним забезпеченням, переваги – виявлення вірусів на ранній стадії, які мінімізують втрати.
- Програми-вакцини – модифікують програми та диски таким чином, що це не впливає на роботу програм, однак вірус вважає їх інфікованими. Вважається, що такий засіб не ефективний, та можуть обмежуватися при застосуванні, тобто використовувати їх можна для знезараження від відомих вірусів.

Антивіруси не можуть гарантувати цілковитий захист, тому пропонується дотримуватись загальних правил та користуватись останніми розробками антивірусних лабораторій.

Поширені такі антивірусні програми [16]:

- для Linux: avast!, Bitdefender, ClamAV, F-Prot Antivirus;
- для Windows: avast!, ADinf, AVG, Bitdefender, ClamAV, F-Prot Antivirus, Dr.Web, ESET NOD32, KASPERSKY, Norton.

3.4 Захист інформації в корпоративних комп’ютерних мережах

Термін «кіберзлочинність» може бути використана разом з терміном «комп’ютерна злочинність», і може бути навіть синонімом [28].

Однак, поняття «кіберзлочинність» набагато ширше, за «комп’ютерну злочинність», і відображає природу даного явища, ніж просто злочинність в інформаційному просторі. Тлумачний словник Оксфордського університету використовує приставку «cyber» - як компонент складного слова. Значення має

відношення до інформаційних технологій, мережі Інтернет, віртуальної реальності, подібне визначення надає і Кембриджський словник [28].

«Cybercrime» – це злочинність, яка пов'язується із застосуванням комп'ютерів із застосуванням інформаційних технологій та глобальних мереж. Тоді як, термін «computer crime» має відношення до шахраїв, які скоюють проти комп'ютерів чи комп'ютерних даних [28].

Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша інформація фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загроза не лише на національному, а й на глобальному рівні [28].

Найпоширенішими видами таких злочинів є [6]:

- Кардинг – застосування в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних та розрахункових систем та з персональних комп'ютерів.
- Фішинг – вид шахрайства, згідно якого клієнтам платіжних систем надсилаються повідомлення електронною поштою начебто від адміністрації чи служби безпеки даної системи з проханням вказівки рахунків та паролей.
- Вішинг – вид кіберзлочинів, де надходить повідомлення про прохання зателефонувати на деякий міський номер, і вже у процесі телефонної розмови намагаються отримати від користувача з конфіденційною інформацією.
- Онлайн-шахрайство – несправжні інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.
- Прості поради для користувача – не передавати персональні дані, паролі та коди-підтвердження з смс-повідомлення для операцій з картками, не довіряти повідомленням про участь/виграші в лотереях, не завантажувати в інтернеті незрозумілі файли, користуватись лише ліцензійним програмним забезпеченням тощо. Але користувачі, все одно допускають такі помилки та потрапляють у казусні ситуації, які призводять до проблем.
- Небанальні. Номер телефону можна здійснити перевірити на сайті кіберполіції, чи звернутися до спеціалістів з проблемою. Кіберполіція

намагається інформувати користувачів, щоб не потрапити в халепу.

- WI-FI – це сервіс, котрий не є захищеним, та має слабкості, так як через нього можна отримати доступ до будь-якого пристрою, підключившись та отримавши інформацією в злочинний цілях. Варто звернути увагу до якої мережі Ви підключаєтесь, чи вона відкрита чи закрита, хто саме займається її роздачею.

Так як зростає кількість публікацій та компаній, котрі професійно займаються забезпеченням захисту інформації в комп'ютерних системах, вирішення даної задачі звертається велике значення. Так як, очевидною причиною для порушення системи захисту та навмисний несанкціонований доступ (НСД) до конфіденційної інформації зі сторони нелегальних користувачів та наступні небажані маніпуляції із цією інформацією.

Захист інформації – це діяльність задля запобігання витоку, викрадення, втрати, редагування, несанкціонованих та ненавмисних впливів на інформацію. Технічні та ненавмисні причини, у процесі визначення підпадає діяльність, яка пов'язується з підвищенням надійності сервера через відмову чи збоїв у роботі вінчестерів, недоліками у застосованому програмному забезпеченні чи інше [6].

Несанкціонований доступ до інформації, який знаходиться у локальних мережах вважається [6]:

- непрямим – без фізичного доступу до елементів локальних мереж;
- прямим – з фізичним доступом до елементів локальних мереж.

Наразі є кілька шляхів несанкціонованого отримання інформації, так звані канали витоку інформації [31]:

1. застосування підслуховуючих пристроїв;
2. дистанційне фотографування;
3. перехоплення електромагнітних випромінювань;
4. розкрадання носіїв інформації і виробничих відходів;
5. зчитування даних у масивах інших користувачів;
6. копіювання носіїв інформації;
7. несанкціоноване використання терміналів;

8. маскування під зареєстрованого користувача за допомогою розкрадання паролів та інших реквізитів розмежування доступу;

9. використання програмних пасток;

10. отримання даних, що захищаються за допомогою серії дозволених запитів;

11. використання недоліків мов програмування і операційних систем;

12. умисне включення в бібліотеки програм спеціальних блоків типу «троянських коней»;

13. незаконне підключення до апаратури або ліній зв'язку обчислювальної системи;

14. зловмисним виведення з ладу механізмів захисту.

Для вирішення проблеми захисту інформації, основними засобами, використовуваними для створення механізмів захисту, прийнято вважати [31]:

- Технічні засоби – електричні, електромеханічні, електронні пристрої.

Переваги технічних засобів пов'язуються з надійністю, незалежністю та стійкістю від модифікації.

Недоліками – є недостатня гнучкість, великий об'єм та висока вартість.

Технічні засоби розподіляються на:

- апаратні пристрої – вбудовуються в апаратне забезпечення, яке підключається до локальних мереж за стандартним інтерфейсом;
- фізичні – реалізуються у вигляді автономних пристроїв та систем.
- Програмні засоби – програми, які призначаються для здійснення функцій, котрі пов'язуються із захистом інформації. Програми для ідентифікації користувачів, контролю доступу, шифрування інформації, тестового контролю системи захисту та ін.

Переваги – універсальність, гнучкість, надійність, простота встановлення, здатність до модифікації та розвитку.

Недоліки – обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів.

- Змішані апаратно-програмні засоби – наділені функціями, які апаратні та програмні, але мають проміжні властивості.
- Організаційні засоби складаються з організаційно-технічних та організаційно-правових.

Переваги – дозвіл для вирішення великої кількості різних проблем, які досить прості в реалізації, при цьому швидко реагують на небажані дії в мережі, але мають необмежені можливості модифікації та розвитку.

Недоліки – висока залежність від суб'єктивних чинників.

У процесі розвитку концепції захисту інформації спеціалісти із захисту інформації призводить до висновку, як використання вищеописаного способу захисту, не забезпечує надійне збереження інформації. Варто все ж звертати увагу на впровадження комплексного підходу щодо застосування та розвитку всіх засобів та способів захисту інформації.

Ступінь поширення та доступність на першому місці використовуються програмні засоби, тому їм і приділяється найбільша увага [31].

Засобами, які застосовуються у випадках, коли слід забезпечити додатковий рівень захисту інформації [31].

Програмними засобами захисту інформації в локальних мережах виділяються [31]:

1. засоби архівації даних – засоби, які реалізовують злиття кількох файлів чи каталогів в один файл. Архів таким чином може зменшити об'єм, при цьому не втрачаючи саму інформацію, яка знаходиться в ньому;

2. антивірусні програми – програми, які розробляються для захисту інформації від вірусів;

3. криптографічні засоби – засоби, які можуть забезпечити конфіденційність, використовуючи шифрування та автентифікацію; засоби ідентифікації та автентифікації користувачів. Автентифікація – перевірка

належності суб’єкта доступу до пред’явленого ним ідентифікатору та підтверджуючи його достовірність. Тобто, автентифікація це перевірка суб’єкту на відповідність його ідентифікатору. Ідентифікація забезпечує реалізацію встановлення автентичності та визначення повноважень суб’єкту при його допуску в систему, контроль за встановлених повноважень у процесі сеансу роботи, реєстрації дій та ін.

4. засоби керування доступом – засоби, які мають певні обмеження та реєстрація входу-виходу об’єктів за заданою територією через «точки проходу»;

5. протоколювання та аудит, де протоколювання забезпечує збір та накопичення інформації щодо події, які відбуваються в інформаційній системі. Аудит – це процес аналізу накопиченої інформації. Мета комп’ютерного аудиту – це контроль відповідності системи чи мережі необхідним за вказаними правилами безпеки, принципами чи індустріальних стандартам.

Аудит забезпечує аналіз щодо проблем безпеки, чи те, що призводить до проблем захисту [24].

Вбудовані засоби захисту інформації в мережевих ОС доступні, але не можуть у повному обсязі вирішити проблеми. Як приклад, це може бути мережна ОС NetWare 3.x, 4.x, котра надає можливість здійснити надійний «захист» даних від апаратних збоїв чи пошкоджень [24].

Система SFT (System Fault Tolerance) компанії Novell, яка включає три основні рівня [24]:

1. SFT Level I – створення додаткових копій FAT та Directory Entries Tables, де здійснюється верифікація кожного файлу на файловий сервер блоку даних та резервування пам’яті на жорсткому диску. У разі виявлення збою, то дані направляються у зарезервовану область диска, та збійний блок позначається як «не хороший», а в подальшому не використовується.

2. SFT Level II – створення «дзеркальних дисків» та копіювання дискових контролерів, джерел живлення та інтерфейсних кабелів.

3. SFT Level III – застосування в локальній мережі дубльованих серверів, де один є пріоритетним, а другий використовується у разі виходу головного сервера з ладу.

Система контролю та обмеження прав доступу в комп'ютерних мережах містить кілька рівнів [24]:

- рівень початкового доступу (входить ім'я та пароль користувача, система облікових обмежень (дозвіл чи заборону роботи), допустимий час роботи в мережі, де місце на жорсткому диску, займане особистими файлами даного користувача);
- рівень прав користувачів (обмеження чи надання доступу на виконання конкретних операцій та/чи на роботу даного користувача, як члена підрозділу, де певних частинах файлової системи мережі);
- рівень атрибутів каталогів і файлів (обмеження на реалізацію окремих операцій (видалення, редагування чи створення), які йдуть з боку файлової системи та стосуються всіх користувачів, які намагаються працювати з каталогами чи файлами);
- рівень консолі файл-сервера (блокування клавіатури файл-сервера на час відсутності мережевого адміністратора до введення ним пароля).

Спеціалізоване програмне забезпечення забезпечує захист інформації від несанкціонованого доступу, яке володіють спеціальними можливостями та характеристиками, а ніж вбудовані засоби мережевих ОС. Окрім програм зашифрування та криптографічних систем, реалізовано велику кількість доступних зовнішніх засобів захисту інформації, то використовуються дві системи, які дозволяють у комплексному підході обмежити та контролювати інформаційні потоки [25]:

- Firewalls – брандмауери, же між локальною та глобальною мережею формується спеціальний проміжний сервер, який перевіряється та фільтрується весь трафік мережевого/транспортного рівнів, який проходить через них. Це дозволяє знизити загрози несанкціонованого доступу, які надходять ззовні в корпоративній мережі, але не вирішує проблему цілковито. Захищений вид

методу – це маскарад, тоді як весь трафік виходить з локальної мережі та надсилається від імені firewall-сервера, реалізуючи майже невидиму локальну мережу практично.

- Proxy-сервери – забороняють весь можливий та потенційний трафік мережевого/транспортного рівнів між локальною і глобальною мережами, тобто маршрутизація відсутня, а звернення з локальної мережі в глобальну здійснюється через спеціальні сервери-посередники. Тому, при зверненні з глобальної мережі в локальну неможливі за будь-яких умов. Даний метод не надає достатнього захисту проти атак на більш високих рівнях.

Реагування на інциденти та відновлення після кібератак в корпоративних мережах - це критично важливий процес для забезпечення безпеки та надійності інформації в організації.

Ось деякі основні методи, які можна використовувати в цьому відношенні:

1. Перш за все, необхідно визначити та класифікувати інцидент. Це допоможе зрозуміти масштаб проблеми та прийняти відповідні заходи.

2. Негайно зупиніть розповсюдження атаки та ізолюйте заражені системи для запобігання подальшому поширенню.

3. Проведіть ретельний аналіз причин та методів атаки, щоб уникнути майбутніх випадків.

4. Відновіть дані та системи за резервними копіями, якщо такі є, або використовуйте інші методи відновлення.

5. Покращіть захист мережі шляхом впровадження нових заходів безпеки та оновлення систем безпеки.

6. Проведіть навчання та свідомості серед персоналу про правила безпеки та процедури реагування на інциденти. Ці методи допоможуть організації ефективно відреагувати на кібератаку та швидко відновити нормальне функціонування корпоративної мережі.

Висновки до розділу 3

У третьому розділі кваліфікаційної роботи було проаналізовано технічні заходи у сфері забезпечення інформаційної безпеки на підприємстві, запропоновано реалізацію захисту інформації на мережевому рівні та засоби і методи захисту від мережевих комп'ютерних загроз. Та на основі вище проведених досліджень запропоновано реалізацію захисту інформації в комп'ютерних мережах.

Тобто, перераховано ключові засоби захисту інформації, їх технічні заходи, проблемами інформаційної безпеки у сфері технічного захисту інформації:

Визначено, що саме використовується для захисту мереж, що для інтеграції засобів програмно-технічного захисту в мережі та можливі варіації.

Види злочинів та несанкціонований доступ до інформації, який знаходиться у локальних мережах, перераховано шляхи несанкціонованого отримання інформації.

Запропоновано спеціалізоване програмне забезпечення забезпечує захист інформації від несанкціонованого доступу, яке володіють спеціальними можливостями та характеристиками, а ніж вбудовані засоби мережевих ОС. Окрім програм зашифрування та криптографічних систем, реалізовано велику кількість доступних зовнішніх засобів захисту інформації, то використовуються дві системи, які дозволяють у комплексному підході обмежити та контролювати інформаційні потоки: брандмауери та proxy-сервери.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

1. Визначенно поняття загроз інформаційної безпеки в корпоративних мережах

2. Поведена класифікація загроз та атак на корпоративні мережі.

3. Розроблено методи захисту від кібератаки в корпоративних мережах.

У першому розділі кваліфікаційної роботи розглянуто аналіз порушень інформаційної безпеки, де визначено рівні інформаційної безпеки, характеристики інформаційної безпеки, типи методів для забезпечення інформаційної безпеки на об’єкті інформаційної діяльності ,методи впливу на інформацію у формі повідомлень.

Проаналізовано основні види мережевих і комп’ютерних загроз, джерела загроз, які впливають на інформацію та протоколи захисту та цілісності IPSec, SSL, TLS.

У другому розділі кваліфікаційної роботи було класифіковано загрози інформації, мережеві атаки та запропоновано методи їх протидії, реалізація безпеки комп’ютерних систем.

Але варто розміти, що захист інформації не має обмежуватися технічними методами. Для ефективного забезпечення інформаційної безпеки варто поєднувати різні моделі та методи оцінки загроз та небезпек.

Інформація є ключовим надбанням та вимагає належного захисту. Тоді як інформація має бути доступною для певного кола користувачів. Тобто, постає питання щодо створення комплексної системи інформаційної безпеки в організації. Дана система має враховувати всі можливі джерела загрози, які були перераховані у розділі, застосовувати весь спектр захисних заходів: фізичних, адміністративних і програмно-технічних засобів захисту.

Окрім цього, розробляються апаратні пристрої для захист мереж на об’єкті інформаційної діяльності. Які успішно використовуються, але незмінними та традиційними залишаються – спеціальне програмне забезпечення.

У процесі вивчення проблем інформаційної безпеки важливо виділити загрози для інформаційної безпеки, аналіз захисту від таких загроз.

Загроза інформаційній безпеці – явище, події від негативних чинників чи процес, де соціальні об’єкти інформаційної безпеки частково чи повністю втрачають можливість реалізувати власні інтереси в інформаційній сфері; порушення стандартного функціонування, здійснення руйнування та стримання розвитку технічних об’єктів інформаційної безпеки.

Безпека комп’ютерних мереж – це досить складне питання для кожної організації, котра включає у собі великий перелік аспектів комп’ютерних технологій, мереж управління, застосування мережі та їх підтримка. Задля підвищення безпеки комп’ютерної мережі варто займатися розробкою ефективних рішень безпеки, заходи для покращення безпеки комп’ютерних мереж. Тому для проходження складного шляху, варто забезпечити нормальну роботу мережевої комп’ютерної системи для об’єкту інформаційної діяльності.

У третьому розділі кваліфікаційної роботи було проаналізовано технічні заходи у сфері забезпечення інформаційної безпеки на підприємстві, запропоновано реалізацію захисту інформації на мережевому рівні та засоби і методи захисту від мережевих комп’ютерних загроз. Та на основі вище проведених досліджень запропоновано реалізацію захисту інформації в комп’ютерних мережах.

Тобто, перераховано ключові засоби захисту інформації, їх технічні заходи, проблемами інформаційної безпеки у сфері технічного захисту інформації:

Визначено, що саме використовується для захисту мереж, що для інтеграції засобів програмно-технічного захисту в мережі та можливі варіації.

Види злочинів та несанкціонований доступ до інформації, який знаходиться у локальних мережах, перераховано шляхи несанкціонованого отримання інформації.

Запропоновано спеціалізоване програмне забезпечення забезпечує захист інформації від несанкціонованого доступу, яке володіють спеціальними можливостями та характеристиками, а ніж вбудовані засоби мережевих ОС. Окрім програм зашифрування та криптографічних систем, реалізовано велику кількість доступних зовнішніх засобів захисту інформації, де використовуються дві системи, які дозволяють у комплексному підході обмежити та контролювати інформаційні потоки: брандмауери та proxy-сервери.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Method of Protecting Relational Databases Copyright with Cloud Watermark // Proceedings of Academy of Science, Engineering and Technology Volume 3 January 2005 ISSN 1307-6884

2. Douglas Crawford OpenVPN over TCP vs. UDP: what is the difference, and which should I choose URL: https://www.bestvpn.com/openvpn-tcp-vsudp-difference-choose/ , 2013.

3. Top 5 Database Security Threats: https://www.imperva.com/docs/gated/WP_Top_5_Database_Security_ Threats.pdf, 2016.

4. Using Secure Connections: https://dev.mysql.com/doc/refman/5.6/en/secureconnections.html.

5. Богуш В.М., Юдін О.К., Інформаційна безпека держави. К.: «МК-Прес», 2005. 432с.

6. Височенко А. А., Петренко А. Б. Методи захисту баз даних. URL: http://www.bezpeka.com/ru/lib/spec/infsys/art92.html.

7. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб. За заг.ред.проф. Я.Ю.Кондратьєва. К., 2016.

8. Герасименко В. А., Малюк А. А. Основи захисту інформації. М.: Инкомбук, 2017. 540 с.

9. Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є., Політика інформаційної безпеки: підручник. Луганськ: вид-во СНУ ім.. В.Даля, 2009, 300с.

10. Закон України «Про доступ до публічної інформації» від 13.01.2011 за № 2939-VI.

11. Закон України «Про захист інформації в автоматизованих системах» від 5.07.1994 за № 80/94-ВР.

12. Закон України «Про захист інформації в інформаційно-

телекомунікаційних системах» від 31.05.2005 за № 2594-IV.

13. Закон України «Про захист персональних даних» від 01.06.2010 за № 2297-VI.

14. Закон України «Про інформацію» від 02.10.1992 за № 2657-XII.

15. Інформаційне забезпечення професійної діяльності : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2018. – 218 с.

16. Козаченко І. П., Голубєв В. О. Загальні принципи захисту інформації в банківських автоматизованих системах URL: http://www.bezpeka.com/ru/lib/spec/infsys/ art92.html, 2005.

17. Кононова В. О., Грибков С. В., Харкянен О. В. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, С. В. Грибков, О. В. Харкянен. *Вісник Нац. ун-ту "Львівська політехніка"*. 2014. № 806. С. 99–105.

18. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів. Уклад. О.Г. Корченко, Ю.О. Дрейс. Житомир : ЖВІ НАУ, 2018. 280 с.

19. Семкин С. Н., Семкин А. Н. Основи інформаційної безпеки об'єктів обробки інформації: Науг.-практ. посібник. Орел: 2018г. 300 с.

20. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович К. : Вид-во DIRECTLINE, 2019. 714 с.

21. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення. О.К. Юдін. Підручник. К. : НАУ, 2016. 620 с.