Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи

бакалавра

(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Інформаційні технології оцінювання захищеності інформаційно-телекомунікаційних систем»

Виконавець: студент IV курсу, групи КБ-41

_____ **Темчур Богдан Володимирович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Яніна ШЕСТАК	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** **Темчуру Богдану Володимировичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Інформаційні технології оцінювання захищеності інформаційно-телекомунікаційних систем

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Літературні джерела, стандарти оцінювання захищеності мереж, сучасні методи оцінювання захищеності мереж.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Теоретичні аспекти інформаційної безпеки телекомунікаційних мереж, поняття інформаційних загроз та їх види, аналіз стандартів у галузі оцінки захищеності інформаційних систем, тестові інформаційно-технічні впливи, оцінка живучості мереж, міжмережеві екрани, віртуальні приватні мережі, принципи інженерно-технічного захисту інформації, власні рекомендації щодо оцінювання захищеності інформаційно-телекомунікаційних мереж.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність дослідження та розкриття питань пов’язаних із оціненням захищеності інформаційно-телекомунікаційних систем, їх практичним застосуванням у подальших наукових дослідженнях.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ Яніна ШЕСТАК
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Богдан ТЕМЧУР
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022 – 11.02.2022	*виконано*
3	Ознайомлення з теоретичними аспектами інформаційної безпеки телекомунікаційних мереж	12.02.2022 – 24.02.2022	*виконано*
4	Дослідження інформаційних загроз	25.02.2022 – 24.03.2022	*виконано*
5	Аналіз стандартів у галузі оцінки захищеності інформаційних систем	25.03.2022 – 07.04.2022	*виконано*
6	Дослідження тестових інформаційно-технічних впливів	08.04.2022 – 20.04.2022	*виконано*
7	Дослідження живучості мереж	21.04.2022 – 05.05.2022	*виконано*
8	Аналіз програмно-апаратного захисту інформації	06.05.2022 – 20.05.2022	*виконано*
9	Аналіз принципу інженерно-технічного захисту інформації	21.05.2022 – 01.06.2022	*виконано*
10	Формування власних висновків та рекомендацій щодо оцінювання інформаційно-телекомунікаційних мереж	02.06.2022 – 06.06.2022	*виконано*
11	Підготовка до захисту	07.06.2022 – 10.06.2022	*виконано*

Завдання видав _____ Яніна ШЕСТАК
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Богдан ТЕМЧУР
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел. Основний текст займає 57 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 9 рисунків.

Методи дослідження: для написання даної дипломної роботи нами було використано метод наукового аналізу, метод інтерпретації результатів та системний метод. Також нами було використано метод науково-методичного дослідження. За допомогою представлених та використаних нами методів, нами було проведено комплексне дослідження та сформовано основні елементи даного наукового дослідження.

У першому розділі даної роботи нами було використано метод науково-методичного дослідження, за допомогою якого нами було опрацьовано теоретичну базу дослідження, матеріал провідних науковців та сформовано в представлений нами перший розділ. Також у даному розділі ми використовували системний метод, за допомогою якого нами було систематизовано опрацьований матеріал та викладено в послідовності нашого дослідження.

У другому та третьому розділах даної наукової праці нами було використано метод аналізу та метод інтерпретації результатів, за допомогою яких нами було проведено порівняльний аналіз досліджуваних нами питань, сформовано власні висновки та інтерпретовано отримані результати аналізу з нашого дослідження. На основі використаних методів нами було сформовано власні висновки та рекомендації з предмету дослідження та сформовано основні поняття інформаційної безпеки телекомунікаційних систем.

Об’єктом дослідження є процес ознайомлення із загальними поняттями інформаційно-телекомунікаційних систем.

Предметом дослідження є технології оцінювання захищеності інформаційно-телекомунікаційних систем.

У роботі проаналізовані основні поняття інформаційної безпеки телекомунікаційних мереж; досліджені сучасні методи використання технології оцінювання захищеності інформаційно-телекомунікаційних систем; запропоновані власні висновки та рекомендації щодо технології оцінки захищеності інформаційно-телекомунікаційних систем.

Ключові слова : інформаційно-телекомунікаційні системи, оцінювання захищеності, захист даних, інформаційні технології, загрози інформаційній безпеці.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІТКС	-	Інформаційно-телекомунікаційна система
ВВС	-	Взаємодії відкритих систем
АІС	-	Автоматизована інформаційна система
НСД	-	Несанкціонований доступ
ІБ	-	Інформаційна безпека
OSSTMM	-	Open-Source Security Testing Methodology Manual
МЕ	-	Мережевий екран
МЗСП	-	Мережа зв’язку спеціального призначення
СЗСП	-	Система зв’язку спеціального призначення
ОТС	-	Організаційно-технічна система
ІТКМ	-	Інформаційно-телекомунікаційна мережа
ДержСОПКА	-	Державна система виявлення, попередження та ліквідації наслідків комп’ютерних атак
КІІ	-	Критична інформаційна інфраструктура
ІТВ	-	Інформаційний технічний вплив
СЗЗК	-	Система зв’язку загального користування

ЗМІСТ

ВСТУП

Актуальність теми : Закон України «Про телекомунікації» та деякі галузеві нормативно-правові акти встановлюють вимоги щодо інформаційної безпеки телекомунікаційних мереж загального користування з метою запобігання несанкціонованому втручанню в роботу мережі, крадіжці, модифікації, вимкненню або знищенню компонентів мережі, а також крадіжок, знищення, спотворення, блокування, несанкціоноване розкриття інформації та порушення встановлених процедур маршрутизації.

Захищена телекомунікаційна мережа повинна бути захищена від зловмисних і ненавмисних атак, бути надійною, стабільною, гарантувати певний час реагування, доступність послуг та інформації, цілісність останньої та обладнання, точність даних розрахунків.

Інформаційна безпека має бути пов’язана не лише із загрозами кожному елементу чи службі, а й із взаємодією засобів та заходів безпеки в мультимедійному середовищі.

Разом із тим, за умови інтеграції інформаційно-телекомунікаційних технологій повною мірою реалізується наскрізна безпека передачі інформації для різних видів мережевих і телекомунікаційних послуг, кількість та якість яких постійно зростають. Адекватний рівень інформаційної безпеки можна підтримувати за допомогою комплексного підходу, який передбачає створення відповідної мережевої інфраструктури, оскільки вразливі місця в будь-якій частині мережі можуть створювати проблеми для постачальників, операторів і споживачів послуг.

Аналіз останніх досліджень та публікацій: інформаційна безпека телекомунікаційних систем стала предметом вивчення для таких провідних науковців, як: С. О. Довгий, В. В. Величко, О. Я. Савченко, П. П. Воробієнко, В. П. Шувалов, А. Е. Стрижак, С. П. Поленок, Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко та інші.

Метою роботи є проаналізувати інформаційні технології та механізми інформаційної безпеки для оцінювання захищеності інформаційно-телекомунікаційних мереж; запропонувати власні рекомендації щодо оцінювання захищеності мереж.

Для досягнення даної мети необхідно вирішити такі завдання :

- проаналізувати основні поняття інформаційної безпеки телекомунікаційних мереж;
- дослідити сучасні методи використання технології оцінювання захищеності інформаційно-телекомунікаційних систем;
- запропонувати власні висновки та рекомендації щодо технології оцінки захищеності інформаційно-телекомунікаційних систем.

Об’єктом дослідження є процес ознайомлення із загальними поняттями інформаційно-телекомунікаційних систем.

Предметом дослідження є технології оцінювання захищеності інформаційно-телекомунікаційних систем.

Методи дослідження дипломної роботи :

- метод наукового аналізу;
- метод інтерпретації результатів;
- системний метод;
- метод науково-методичного дослідження.

РОЗДІЛ 1
ВИЗНАЧЕННЯ ОСНОВНИХ ПОНЯТЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1. Теоретичні аспекти інформаційної безпеки телекомунікаційних мереж

Інформаційна безпека заснована на багатошарових принципах безпеки. Це значить, що безпека гарантується на кожному рівні моделі ВВС, а відповідні функціональні послуги розподіляються між цими рівнями. Модель ВВС розрізняє сім рівнів обробки інформації [1, с. 187]:

1) фізичний;
2) канальний;
3) мережний;
4) транспортний;
5) сеансовий;
6) представний;
7) прикладний.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рисунок 1.1 - Модель OSI

Кожен рівень виконує певні завдання та функції, сприяючи діяльності на відповідному рівні. У режимі Air Force кожен рівень має окремі засоби, служби та служби. Об’єкти взаємодіють через інтерфейси та протоколи. Послуги, які надає BBC Model Organization. ITI-T стандартизує телевізійні послуги, послуги передачі та послуги безпеки [2, с. 64].

Служби безпеки повинні забезпечувати безпеку системи. Термін «безпека системи» відноситься до стану системи, який мінімізує вразливість ресурсів, доступних у системі. Уразливість – це ослаблення, яка може бути використана для компрометації системи чи інформаційної структури. Загрози є потенційними порушеннями безпеки. ITI-T X.800, який поділяє загрози на свідомі та випадкові, виділяє такі загрози ресурсам інформації у інформаційно-телекомунікаційних системах:

- ♦ зруйнування інформаційних джерел;
- ♦ викривлення або зміна інформації;
- ♦ викрадення, втрата інформаційних ресурсів;
- ♦ розголошення закритої інформації;
- ♦ переривання послуг.

Як тільки загроза буде виявлена, розроблюється завдання для забезпечення безпеки. З точки зору забезпечення інформаційної безпеки набір засобів захисту можна розглядати як сукупність функціональних сервісів, які разом становлять необхідний функціональний профіль захисту. Кожен сервіс – це набір можливостей, які дозволяють захиститися від набору загроз. Служби безпеки мережі побудовані за принципом ієрархічної багаторівневої модульності: служби безпеки – служби безпеки – функціональні служби безпеки - механізми захисту [1, с. 188].

Служби безпеки поділяються на фазу зв'язку та рівень ВПС. Існують відмінності в застосуванні однієї і тієї ж послуги на різних рівнях. За запитом певні послуги безпеки не потрібні. Конкретні послуги надаються на кількох рівнях.

Політика безпеки для кожної служби може бути реалізована за допомогою різних механізмів безпеки (окремо або в комбінації) залежно від об’єкта політики. Сервіси фізичного рівня є основою. Метою захисту фізичного рівня є належний

захист фізичного потоку бітів даних (служба класифікації з’єднань) та забезпечення конфіденційності трафіку (служба класифікації потоків даних). Захист фізичного рівня здійснюється за допомогою шифруючого обладнання [2, с. 65].

Послуги фізичної безпеки можуть використовуватися окремо або в комплексі. Наприклад, при дуплексній одночасній двоточковій передачі можна забезпечити повну конфіденційність з’єднання. Для інших типів передач, таких як асинхронні передачі, можна досягнути лише невеликої конфіденційності підключення. Служби безпеки на рівні мережі дуже важливі.

Протокол мережевих служб ВВС для доступу, підключення та маршрутизації мережі використовує механізми безпеки. В інформаційній безпеці інформаційно-телекомунікаційних мереж виділено наступні механізми безпеки [2, с. 66]:

♦ Конфіденційність (методики криптографії та шифрування), яка повинна гарантувати, що технічна інформація мережі та дані споживачів будуть недоступними та не розкритими користувачам, які не мають необхідних дозволів. Крім того, навіть коли використовуються відкриті засоби захисту, необхідно забезпечити захист конфіденційності системної інформації з дати встановлення;

♦ цифровий підпис;

♦ контроль доступу, який повинен визначати дозволений набір операцій для кожного об'єкта та контролювати дотримання цих специфікацій;

♦ механізми (сервіси) цілісності даних, які повинні забезпечувати цілісність, точність і надійність інформації, що передається по мережі, та даних споживачів, що зберігаються в мережевій базі даних;

♦ перевірка ідентичності – визначення автентичності інтерактивного суб'єкта на основі інформації про особу, наданої інтерактивним суб'єктом;

♦ заповнення трафіку;

♦ контроль маршрутизації;

♦ послуга аутентифікації об'єктів 1 рівня – забезпечується шляхом обміну механізмами безпечної аутентифікації (захищеного пароля) та цифрового підпису;

♦ служби аутентифікації походження даних – механізми шифрування або підпису;

♦ послуга таємності з’єднання – механізми шифрування та/або контроль маршрутизації;

♦ послуги конфіденційності без з'єднання – механізми керування шифруванням та/або маршрутизацією;

♦ служба прихованості трафіка – механізм для заповнення трафіку контекстною інформацією на рівні мережі або каналу та/або керування маршрутизацією разом із Службою конфіденційності;

♦ використовувати механізми цілісності даних для надання послуг цілісності з'єднання без відновлення, іноді в поєднанні з механізмами шифрування;

♦ надання послуги забезпечення цілісності без використання механізмів цілісності даних, іноді в поєднанні з механізмами шифрування [2, с. 67].

Архітектура інформаційної безпеки телекомунікаційної мережі підтримує комплексну (зверху-вниз і наскрізь) мережеву безпеку елементів, послуг і додатків, виявляючи, прогнозуючи та виправляючи порушення безпеки [1, с. 190-191].

Захищені всі компоненти телекомунікаційної мережі: лінії, канали, системи передачі, обладнання, програмне забезпечення, інформація та люди. Існує потреба в гармонізації підходів до інформаційної безпеки для різних компонентів телекомунікаційних мереж, особливо інформаційних ресурсів, додатків, телекомунікаційних протоколів. Кінцевою метою є вибір ефективного засобу подолання загроз при впровадженні систем інформаційної безпеки, вартість якого не перевищує очікувану вартість втрат реалізації загрози. Архітектура інформаційної безпеки логічно розділяє складну мережу між її кінцевими точками на окремі компоненти.

Відділ дотримується системного, інтегрованого, наскрізного підходу до інформаційної безпеки для планування безпеки та оцінки кібербезпеки.

Вважається, що архітектура інформаційної безпеки пов’язана з трьома архітектурними компонентами: механізмами безпеки та рівнями та площинами, які вони забезпечують. Механізм інформаційної безпеки — це набір заходів безпеки, який захищає від усіх основних загроз безпеці, підтримує політики безпеки,

визначені для певної мережі, і сприяє дотриманню набору правил управління безпекою [2, с. 68].

Ці заходи, які не обмежуються мережею, а також застосовуються до програм і кінцевих користувачів, вживаються постачальниками послуг або компаніями, які мають ліцензію на діяльність у сфері надання функцій безпеки. Механізмами захисту інформації мережі є: контроль доступу, аутентифікація, недоторканність участі в обмінах, конфіденційність даних, безпека зв'язку. У порівнянні з ITC-T Rec. X.800, новий механізм захисту інформації мережі забезпечує доступність і конфіденційність. Забезпечення доступності означає, що події, які мають вплив на систему, не спричиняють відмови у авторизованому доступі до елементів мережі, інформаційних ресурсів, служб і програм. Забезпечення таємності направлене на захист інформаційних ресурсів, що потенційно можна отримати шляхом моніторингу мережевих операцій [1, с. 192].

Прикладами такої інформації є веб-сторінки, які відвідує користувач, географічне розташування користувача, IP-адреса або назва пристрою BH8 в телекомунікаційній мережі постачальника послуг. Слід зазначити, що державні документи у галузі захисту інформаційних технологій не визначають механізмів гарантування власності, що, можливо, є наслідком відсутності в нашій державі звичаю незайманості приватної власності. Проте Конституція України, Закон України «Про телекомунікації» (стаття 9), положення про ліцензії та інші нормативно-правові акти передбачають норми захисту конфіденційності зв'язку «для забезпечення конфіденційності інформації щодо споживачів, договорів, наданих телекомунікаційних послуг, тривалість послуги, зміст, спосіб оплати, шлях передачі тощо».

Навіть якщо в договорі не обговорено надання послуг із забезпечення конфіденційності інформації про споживача, повинні існувати механізми для забезпечення конфіденційності такої інформації. Механізми інформаційної безпеки використовуються для боротьби з різноманітними загрозами. З метою забезпечення наскрізної безпеки інформаційно-телекомунікаційних мереж механізми для надання

безпеки поєднуються в рівні безпеки. Далі, на кожному з цих рівнів є декілька видів механізмів інформаційної безпеки - площина інформаційної безпеки [1, с. 193].

Існують такі системні рівні мережево-орієнтованих засобів гарантування безпеки інформації: рівень гарантування безпеки інфраструктури, рівень гарантування безпеки інформації послуг, рівень гарантування інформаційної безпеки застосувань. У Рекомендації ITRG-T X.805 прописано, що всі три перелічені рівні інформаційної безпеки можуть бути використаними на кожному із семи рівнів моделі ВВС, оскільки вона має власну інфраструктуру, яка забезпечує чітко визначені послуги та програми [2, с. 69].

Рівень інформаційної безпеки програми концентрується на безпеці мережевих програм, доступних клієнтам постачальника послуг. Ці програми дають змогу мережевим службам і центрам обробки даних виконувати передачу ресурсів і функції додатків, функції керування довідкою, голосом та електронною поштою, а також розширені функції, як, наприклад, управління телекомунікаціями споживачів, навчання на відстані, відеозустрічі та багато іншого. На рівні існують потенційні цілі атаки на безпеку: програми користувачів, програми постачальників і постачальники послуг.

Площина інформаційної безпеки – система безпеки інформації, що працює в захищеній мережі. Визначено три рівні інформаційно-телекомунікаційної безпеки, що відповідають трьом операціям безпеки в мережі: рівень управління безпекою, рівень контролю безпеки та сигналізації та рівень безпеки фінального споживача. Ці площини показують особливі потреби безпеки інформації і стосуються реалізації управління мережею, організації управління мережею та сигналізації кінцевих користувачів. Мережі мають бути спроектовані таким чином, щоб процеси в одній площині безпеки були не залежними від процесів у інших рівнях безпеки [29, с. 70].

Наприклад, хвиля запитів кінцевих користувачів до служб доменних імен (BM8) не повинна перешкоджати інтерфейсу керування, адміністрування, обслуговування та підтримки (OAM&R), щоб адміністратори могли приймати правильні рішення.

Кожний тип функцій системи, що були представлені, має специфічні потреби гарантування безпеки. Структура площин інформаційної безпеки надає можливість диференціювати особливості безпеки відносно різних дій, що пов’язані з цими площинами, оцінюючи їх самостійно, окремо одну від одної [1, с. 194].

Площина керування забезпечує функції надійності, працездатності та безпеки (PCAP8). Підмережі, які передають трафік для зручності керування, можна використовувати за межами користувацького трафіку.

Методологічний підступ до безпеки інформаційно-телекомунікаційних систем заключається в розгляді кожного окремого механізму захисту на всіх трьох рівнях інформаційної безпеки та також трьох площинах інформаційної безпеки. Таким чином, маємо 9 модулів безпеки, кожен з них має вісім механізмів безпеки, які можуть застосовуватися на окремих рівнях і в окремих площинах.

Також потрібно розуміти, що залежно від потреб певної мережі може стати в нагоді повний або неповний набір механізмів інформаційно-телекомунікаційної безпеки, рівнів і площин інформаційної безпеки. Архітектура інформаційної безпеки має право бути використаною стосовно кожної мережі на будь-якому рівні стеку протоколів [2, с. 71-72].

Прикладний рівень описує безпеку користувацьких програм, доступ до яких здійснюється через мережу e-Thai IP. Аналогічно, для мереж асинхронної передачі (ATM), які розташовані на двох рівнях стеку протоколів, рівень інфраструктури описує окремі комутатори та канали зв'язку «точка-точка» між комутаторами. Рівень обслуговування описує різні класи рекомендованих методів передачі (постійна швидкість передачі, змінна швидкість передачі в реальному часі, доступна швидкість передачі та невизначена швидкість передачі) [2, с. 73].

Нарешті, рівень програми стосується кінцевого користувача, який використовує мережу банкоматів для того, щоб мати доступ до програми для відеоконференцій [1, с. 196-197].

1.2. Поняття інформаційних загроз та їх види

Загрози інформаційній (комп'ютерній) безпеці – це різноманітні дії, які можуть призвести до порушення інформаційної безпеки. Іншими словами, це потенційні події, процеси чи дії, які можуть пошкодити інформацію та комп'ютерні системи. Загрози інформаційної безпеки можна розділити на дві категорії: природні загрози та техногенні загрози. До природних явищ належать ті, які не залежать від людини, наприклад, урагани, повені, пожежі тощо [3, с. 124].

Штучні загрози безпосередньо залежать від людини і можуть бути навмисними або випадковими. Випадкові загрози походять від необережності, недбалості та незнання. Прикладом такої загрози є інсталяція непотрібних для роботи програм і подальше пошкодження системи, що призведе до загублення інформації. На відміну від випадкових загроз, навмисні погрози створюються спеціально. Сюди входять атаки хакерів як "з вулиці", так і з середині фірми або компанії [4, с. 3].

Проблеми інформаційної безпеки хвилюють фахівців з комп'ютерної безпеки та багатьох звичайних користувачів ПК з кінця 1980-х і початку 1990-х років. Це може бути зв'язано з великими перемінами, які інформаційні технології приносять у наше з вами життя.

Новітні автоматизовані інформаційні системи (АІС) – це доволі важкі механізми, які формуються з величезної кількості складових з різним ступенем автономності, взаємозв'язку, обміну даними. Майже кожен може зазнати невдачі або піддатися впливу сторонніх факторів.

Хоча цей метод дорогий, можливості комп'ютерних автоматизованих інформаційних систем змогли показати неміцні місця в інформаційній безпеці. Неминучим наслідком є постійно зростаючі витрати та сили, що спрямовані на поліпшення захисту інформації.

Проте для ефективності вжитих заходів необхідно виявити загрози інформаційній безпеці, можливі канали втрати інформаційних ресурсів та способи незаконного доступу до даних, що захищаються [3, с. 125].

Загроза інформаційній безпеці (інформаційна загроза) – це дія або подія, яка може призвести до знищення, спотворення або несанкціонованого використання інформаційних ресурсів, у тому числі інформації, що зберігається, передається та обробляється, а також програмного та апаратного забезпечення. Існує загроза порушення конфіденційності інформації, якщо цінність інформації буде втрачено під час її зберігання та/або поширення. Загрози цілісності інформації проявляються, якщо інформація змінюється або знищується внаслідок втрати цінності. Якщо інформація вчасно не надходить до законних користувачів, її цінність з часом падає і повністю знецінюється, загрожуючи ефективності чи зручності використання інформації [4, с. 4].

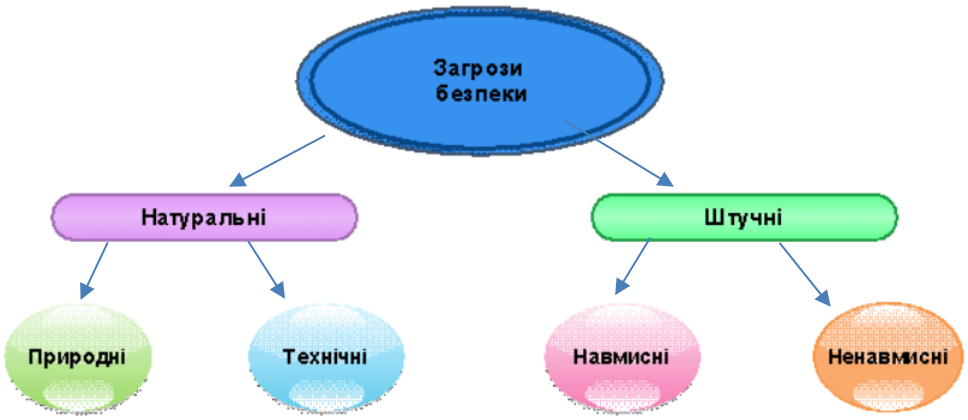

Рисунок 1.2 - Загальна класифікація загроз інформаційній безпеці

Інформаційні загрози виникають через:

- природні чинники (пожежа, повінь, блискавка та подібне);
- фактор людини.

Людські фактори поділяються на:

- Випадкові загрози. Вони стосуються помилок у підготовці, обробці та передачі (науково-технічні, комерційні, грошові та фінансові документи); ненавмисний «витік мізків», знання, інформація (наприклад, пов’язані з імміграцією, поїздками в інші країни, пов’язані з возз’єднаннями сімей, тощо). Це погрози, які

стосуються помилок у роботі обладнання через неякісне виготовлення; помилок у підготовці та обробці інформаційних ресурсів [4, с. 5];

- Погрози, зумовлені навмисними діями людей. Ці загрози пов’язані з перекручуванням, модифікацією наукових винаходів, які створюють секрети, нових технологій (документів, креслень, описів відкриттів) з власних або якихось інших мотивів; прослуховування та передача офіційних та інших діалогів науки, техніки та бізнесу, цілеспрямований «відтік мізків», знання інформації. Це загрози, що стосуються незаконного заволодіння ресурсами автоматизованої системи [3, с. 126].

Умисні загрози можна розділити на активні та пасивні загрози.

Пасивні загрози зазвичай мають на меті несанкціоноване оволодіння інформаційними ресурсами, не впливаючи на їх функціональність. Наприклад, пасивна загроза - це спроба прослухати канал зв'язку, щоб отримати інформацію, яка поширюється в каналі зв'язку.

Активні загрози покликані порушити нормальну роботу систем шляхом спеціального втручання в роботу апаратно-програмних або інформаційних ресурсів. Активні загрози включають, наприклад, саботаж або електронне спотворення ліній для зв'язку, вихід з ладу ПК або його окремих частин, спотворення інформації в інформаційних базах даних та подібне.

Умисні загрози можна умовно розділити на такі, що створюються всередині компанії (внутрішні), та зовнішні.

Інсайдерські загрози часто визначаються соціальною напругою та складним моральним кліматом [3, с. 127-128].

Зовнішні загрози можна визначити через зловмисну поведінку конкурентів, економічні умови та інші причини, такі як стихійні лиха. За даними, які можна знайти в різних джерелах, промислове шпигунство набуло поширення – воно завдає шкоди власникам комерційної таємниці, незаконно збираючи, привласнюючи та передаючи інформацію, що становить комерційну таємницю, причому власники такої інформації роблять це несанкціоновано [4, с. 6].

Загрози викриття таємної інформації можуть бути реалізовані завдяки несанкціонованому доступу до баз даних, де зберігаються інформаційні ресурси,

прослуховуванню каналів, по яких може передаватися інформація та багато іншого. Незаконне заволодіння інформацією, що є особистою власністю певної особи або групи осіб, веде до сильного зменшення цінності даної інформації.

Конфіденційне розголошення – це розкриття таємної інформації за межами кола інтелектуальної власності або осіб, яким довірено чи поінформовано в процесі роботи. Цей витік може бути викликаний:

- Розкриттям конфіденційної інформації;
- Несанкціонованим доступом до закритої інформації багатьма способами.
- Розкриття інформації її власниками є спеціальною чи недбалою поведінкою осіб та споживачів, які доручили відповідну інформацію у встановленому порядку для надання послуг чи роботи, що призвело до знайомства з особами, які не мають доступу до цієї інформації [4, с. 7].

Канал витоку конфіденційної інформації можна описати як шлях від джерела, де зберігається така інформація, до крадія, який може потім розголошувати та розповсюджувати різноманітні відомості, що охороняються і не мають права бути розкритими. Для того, щоб такий канал був створений, потрібні деякі умови в просторі та часі, відповідні механізми зчитування та фіксації інформації з боку крадія.

В цілому канали витоку інформаційних ресурсів можна розділити на такі категорії:

- візуально-оптичні;
- акустичні;
- електромагніті;
- матеріально-речові (наприклад, папір, магнітні носії, тверді, рідкі та газоподібні виробничі відходи).

Візуально-оптичні канали – це чи віддалене або ж близьке (наприклад, телевізійне) спостереження. Фактором, який доносить інформацію, є світло, воно запускається базами даних, де міститься конфіденційна інформація або може бути відображеним у видимому для людського ока інфрачервоному та ультрафіолетовому діапазонах [3, с. 130-131].

Акустичні канали. Цей канал витоку інформації є дуже поширеним, тому що слухом людина сприймає велику кількість інформації. У ньому передавачем інформації є звук, що лежить у смугах ультра, чутного та інфразвукового діапазонів. [4, с. 8].

У вільному просторі, при відкритих дверях, вікнах, під час перемовин у приміщеннях утворюються акустичні канали. З іншого боку, такі повітропроводи утворені системами вентиляції повітря. При цьому формування каналу багато в чому залежить від геометрії і форми воздуховода, формоутворюючих елементів клапана, акустичних властивостей повітророзподільника і подібних елементів.

Електромагнітні канали. У даному випадку передавачем інформаційних ресурсів виступають електромагнітні хвилі в діапазоні від наддовгих, довжина яких складає 10000 м, до сублімованих, які досягають 1 - 0,1 мм. Кожен без винятку вид хвиль має особливості в поширенні у дальності і в просторі. Візьмемо до прикладу довгі хвилі, що поширюються на великі відстані, міліметри – натомість видаляють лише одиниці та лінію видимості в межах десятків кілометрів [3, с. 132].

Матеріальними каналами інформації є різні речовини у вигляді твердих тіл, рідин і газів або частинок (радіоактивних елементів). Переважно це різні обрізки, брак, сировина тощо.

Очевидно, що кожне джерело конфіденційної інформації практично не може бути убезпеченим від наявності каналів витоку інформації.

Причин таких витоків є багато, але в основному вони стосуються недовершеності правил збереження конфіденційної інформації, а також недотримання цих правил, неправильним поводженням із певними документами, технічними засобами, матеріалами, що містять деякі кількість конфіденційної інформації [4, с. 9].

Фактори витоку можуть включати, наприклад:

- недостатнє розуміння та нерозуміння співробітниками компанії правил захисту інформації, яких зобов’язаний дотримуватися кожен;
- недостатній рівень контролю за дотриманням правил збереження за допомогою правових, організаційних та інженерних заходів;

- несанкціонований доступ (UID)

Це найпоширеніший вид інформаційної загрози, коли користувач отримує доступ до об’єктів, до яких не має доступу відповідно до прийнятих в організації політик безпеки. Часто головна проблема полягає в тому, щоб зрозуміти, хто і до якого переліку даних повинен мати доступ, а хто не повинен. Тобто, треба визначити, що означає термін «несанкціонований».

Можна сказати, що дії НСД є впливом, який має на меті виявлення та використання помилок, що виникають у системі. Несанкціонований доступ в основному звертається особисто до набору даних, який є необхідним, або впливає на інформацію про санкціонований доступ для того, щоб легалізувати НСД. НСД може бути здійснений різними програмними засобами : стандартними або ж такими, що розроблюються спеціально для об'єктів [4, с. 10].

Проте не треба забувати і про доволі примітивні способи несанкціонованого доступу:

- розкрадання носіїв інформації;
- ініціативне співробітництво;
- випитування;
- підслуховування;
- спостереження та інші шляхи.

Будь-яке розголошення конфіденційної інформації потенційно може завдати істотної матеріальної та моральної шкоди організації, в якій функціонує об’єкт інтелектуальної власності, та її користувачам [3, с. 133-134].

Керівники повинні ніколи не забувати, що більша частина чинників та умов, які створюють передумову та можливість незаконного привласнення конфіденційної інформації, випливають із фундаментальних недоліків керівництва організації та її співробітників. Наприклад, причини та умови, які є передумовою для розголошення комерційної таємниці, можуть включати:

- недостатня обізнаність працівників організації про правила захисту конфіденційної інформації та необхідність їх суворого дотримання;

▪ використання неавтентифікованих технічних засобів для обробляння конфіденційної інформації;

▪ погане контролювання, таке як правова організація та інженерні заходи щодо дотримання правил захисту інформації.

У програмному забезпеченні АІС можуть виникати різні помилки, якщо таке трапляється, то на виході можна отримати розкриття або компрометацію інформаційних ресурсів, які є таємними і не повинні бути розголошеними.

У контексті кримінального законодавства одночасна передача інформаційних ресурсів на інший технічний носій не буде вважатися знищенням комп'ютерної інформації за умови, що такі дії істотно не перешкоджають або не перешкоджають доступу до інформації законним користувачам.

Можливість використання програмного забезпечення для відновлення пошкодженої інформації або отримання цієї інформації від інших користувачів не повинна звільняти винну особу від відповідальності [3, с. 135].

Також винищенням інформації не вважається зміна назви файлу, де вона знаходиться, а також витискання старих версій файлів, що застаріли, яке є зазвичай автоматичним.

Блокування комп'ютерної інформації – це ускладнення для користувачів, що утворюється штучно, щоб отримати комп'ютерну інформацію, і не має нічого спільного з ліквідацією комп'ютерної інформації. Сформувавши по-іншому – це доручення інформації в результаті неможливості отримати або використати інформацію за призначенням із повною безпекою самої інформації [4, с. 11].

Як правило, витік інформації досягається шляхом внесенням незаконних змін у базу даних, тому її споживачі змушені або відмовлятися від неї, або наполегливо працювати, щоб виявити зміни та відновити правдиву інформацію. Якщо використовується компрометована інформація, споживачі ризикують прийняти неправильне рішення з подальшими відповідними наслідками.

Відмова від фактичної інформації, у тому числі і непризнання банківської транзакції означає невизнання одержувачем або відправником даної інформації фактів її отримання чи відправлення відповідно. Якщо взяти до прикладу

маркетингову діяльність, то це може дозволити відправнику або одержувачеві розривати фінансові угоди, що були вже між ними заключені, "технічним" шляхом, тобто формально не відмовляючись від них, але завдаючи цим іншій людині немалих збитків.

Модифікація комп'ютерної інформації – це факт видозмінення деякої інформації, але якщо воно не включає зміни в адаптації програми для ЕОМ або змін у базах даних. Адаптація комп’ютерної програми чи бази даних – це «модифікація, внесена лише для забезпечення того, щоб комп’ютерна програма чи база даних працювала за допомогою спеціальних технічних засобів користувача або під керівництвом конкретної програми користувача». Тобто, можна прийти до висновку, що зміст програми або бази даних змінився, якщо порівнювати з тим, що спершу був доступний власнику або законному користувачу [3, с. 136].

Відтворення комп'ютерної інформації – створення та стабільне відображення другої та наступних копій баз даних або файлів у будь-якій матеріальній формі та їх записів на машинних носіях у пам'яті комп'ютера.

Якщо говорити про відмову в обслуговуванні, то вона є важливою та поширеною загрозою, джерелом якої може виступати сама АІС. Така відмова є занадато небезпечною в ситуаціях, коли затримка надання ресурсів абонентам може мати серйозні наслідки. До прикладу, якщо користувач не має тих даних, що необхідні йому для прийняття правильного рішення прямо зараз, або протягом періоду, коли воно (рішення) ще може бути реалізовано ефективно, то це в майбутньому може вилитися в нераціональні дії даного користувача, які матимуть непередбачувані наслідки [4, с. 12].

1.3. Аналіз стандартів у галузі оцінки захищеності інформаційних систем

Проблема тестування та оцінки засобів гарантування інформаційної безпеки (ІБ), оцінки захищеності автоматизованих систем (АС) є на сьогоднішній день актуальною, що підтверджується аналізом вітчизняних та зарубіжних стандартів у

цій галузі. Важливим елементом оцінки стану безпеки є тестування як підтвердження того, що засоби захисту відповідають стандартам та функціонують коректно [5, с. 84].

Стандарти ІБ є основним критеріальним засобом, який використовується для вирішення прикладних завдань забезпечення безпеки АС. Як основні стандарти в галузі формування вимог до засобів захисту, їх оцінки та тестування можна виділити такі документи:

1. Керівні документи, зокрема: «Керівний документ. Кошти обчислювальної техніки. Міжмережеві екрани. Захист від несанкціонованого доступу до інформації. Показники безпеки від несанкціонованого доступу до інформації».

2. Загальні критерії безпеки інформаційних технологій і автентичний йому ДСТУ ISO 15408-2002;

3. Open-Source Security Testing Methodology Manual (OSSTMM), ISECOM-методологія тестування безпеки;

4. Guideline on Network Security Testing, NIST Special Publication 800-42 – практичний посібник із тестування мережевої безпеки. Далі дані стандарти та положення розглядаються з точки зору їх застосування до процесу тестування міжмережевих екранів [6, с. 61].

У документі встановлено п'ять класів захищеності МЕ, класифікованих за рівнем захищеності від несанкціонованого доступу (НСД) до інформації з урахуванням переліку показників захищеності.

Кожен клас характеризується певною мінімальною сукупністю вимог щодо захисту інформації. Для АС класу 3А, 2А залежно від важливості оброблюваної інформації повинні застосовуватися МЕ наступних класів:

- при обробці інформації з грифом секретно – не нижче 3 класу;
- при обробці інформації з грифом «цілком секретно» – не нижче 2 класу;
- при обробці інформації з грифом «особливої важливості» – не нижче 1 класу.

До показників захищеності віднесено:

– Управління доступом;

– Адміністрування: ідентифікація та аутентифікація;

– Реєстрація;

– Цілісність;

– Відновленість;

– Тестування;

– Управління адміністратора захисту;

– Документація для тестування;

– Конструкторська (проектна) документація. До мінусів керівництва можна віднести жорсткість і статичність показників захищеності, відсутність гнучкості у підході оцінки (основний акцент для формування вимог робиться забезпеченні конфіденційності і цілісності інформації) [6, с. 62].

Якщо клас екрана третій і вище, необхідно переконатися, що він працює на рівні програм для всіх програм, що використовуються в процесі зовнішнього інформаційного обміну. Крім того, класифікація АС і СВТ розроблялася без урахування розподіленої архітектури сучасних АС, а практично всі сучасні комерційні МЕ за своїми можливостями суттєво перевищують вимоги 1-го класу захищеності (за винятком вимог щодо використання сертифікованих криптографічних алгоритмів) [5, с. 85-86].

«Загальні критерії»

Цей стандарт пропонує підходи, методи та функції забезпечення захисту інформації. Також як і РД Держтехкомісії "Загальні критерії" використовуються для проведення сертифікаційних випробувань. "Загальні критерії" являють собою методологію формування вимог оцінки безпеки. Оцінка інформаційної безпеки базується на моделях (профілях) безпеки, що складаються з перерахованих у стандарті функцій. Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації.

Усі функції представлені у вигляді чотирьохрівневої ієрархічної структури: клас – сімейство – компонент – елемент. За аналогією представлені вимоги якості. У стандарті виділено 11 класів функцій: аудит, ідеентифікація та аутентифікація, криптографічний захист, конфіденційність, передача даних, захист даних, управління безпекою системи, використання ресурсів, доступ до системи, надійність

засобів. ISO 15408 містить ряд визначених профілів, що описують стандартні модулі системи безпеки (наприклад, профіль міжмережевого екрану) [5, с. 87].

Таким чином, «Загальні критерії»:

– дозволяє визначити повний перелік вимог до засобів безпеки, а також критерії їхньої оцінки (показники захищеності інформації);

– дозволяє провести оцінювання стосовно того, наскільки наповнена система інформаційної безпеки з точки зору технічної, але при оцінюванні не беручи до уваги повний комплекс заходів щодо гарантування інформаційного захисту.

Методологія тестування безпеки (OSSTMM)

Рисунок 1.3 – Емблема OSSTMM

Цей документ містить загальну методологію та пропонує практичні рекомендації щодо організації процесу тестування безпеки: формує базові визначення, виділяє об'єкти тестування, пропонує шаблони документів для проведення тестів. У OSSTMM виділено такі категорії безпеки, які взаємопов'язані одна з одною:

– інформаційна безпека (information security)

– безпека процесу (process security)

– безпека Інтернет-технологій (internet technology security)

– безпека комунікації (communications security)

– бездротова безпека (wireless security)

– фізична безпека (physical security)

Перелічені вище категорії розбиті на модулі [6, с. 63-64].

Процес тестування є безперервним і проходить через усі модулі та категорії. В рамках тестування одного модуля виділяють збір даних «data» (робиться припущення про певну властивість системи) та перевірку зробленого припущення «verification». Дані, отримані в результаті тестування одного модуля можуть бути як кінцевим результатом, так і вихідними даними для тестування наступного модуля. Тестування міжмережевих екранів віднесено до категорії безпеки Інтернет-технологій.

Крім того, в рамках модуля безпеки Інтернет-технологій можна виділити моделі, результати тестування яких будуть використовуватися для проведення тестування міжмережевих екранів:

– сканування портів;

– ідентифікація систем та сервісів;

– пошук уразливостей;

– тестування маршрутизації;

– злом паролів;

– аналіз стійкості до атак (у тому числі атак типу «відмови в обслуговуванні»).

До очевидних недоліків даної методології можна віднести: відсутність рекомендацій щодо формування системи вимог до засобів захисту інформації, а також відсутність рекомендацій щодо вибору та використання інструментів для тестування. Крім того, перерахованих вище підходів недостатньо для оцінки ефективності функціонування засобів захисту та оцінки захищеності АС.

Посібник із тестування мережевої безпеки (NIST) [5, с. 88].


DRAFT Guideline on Network Security Testing

Recommendations of the National Institute of Standards and Technology

COMPUTER SECURITY

Рисунок 1.4 - NIST 800-42

Цей стандарт дає практичні рекомендації щодо організації процесу тестування мережевої безпеки; визначає ролі, інструменти та стадії життєвого циклу, на яких необхідно виконувати тестування. Об'єктами мережевої безпеки, згідно з документом, є міжмережеві екрани, маршрутизатори та комутатори, сервери різного призначення (Web, Email, DNS, FTP та інші) [6, с. 65].

Життєвий цикл цих об'єктів є класичною схемою: формування вимог, розробка (придбання), використання, експлуатація, виведення з дії. Тестування властивостей безпеки необхідно виконувати на стадіях впровадження (при виборі пристрою) та експлуатації (для оцінки захищеності та коректності роботи). У документі розглядаються різні підходи щодо оцінки мережевої безпеки, зокрема:

– сканування мережі (network mapping)

– сканування вразливості (vulnerability scanning)

– злом пароля (password cracking)

– аналіз лог-журналів (log review)

– перевірка цілісності файлів (file integrity checkers)

– тестування на проникнення (penetration testing)

Дані методи можуть застосовуватися для тестування міжмережевих екранів як окремо, так і комплексно. Так сканування вразливостей завжди включає в себе сканування мережі (визначення відкритих портів, ідентифікація систем), а тестуванню на проникнення передує пошук (сканування) вразливостей [5, с. 89].

Стандарт «Guideline on Network Security Testing» є хорошим практичним посібником для організації процесу оцінки стану мережевої безпеки, проте документ не містить вимоги до засобів мережевої безпеки, на відповідність яких необхідно проводити тестування.

Стандарти з оцінки безпеки практично не містять конкретних методик, внаслідок чого величина розриву між загальними деклараціями та конкретним інструментарієм щодо реалізації та контролю їх положень є неприпустимою. Аналіз зарубіжних та сучасних вітчизняних стандартів в області ІБ показує, що їхнє успішне застосування вимагає розробки додаткових спеціальних методів,

алгоритмів та методик оцінювання захищеності та проведення процесу тестування [6, с. 66-67].

Висновки за розділом 1

Отже, з проведеного нами дослідження в першому розділі, можемо зробити такий висновок, що рівень інформаційної безпеки інфраструктури телекомунікаційної мережі складається із засобів мережі передачі інформації та різних елементів мережі та захищається механізмом захисту інформації. Рівень інфраструктури складається з основних блоків систем, сервісів і додатків. Прикладами компонентів на рівні інфраструктури є окремі маршрутизатори, комутатори та служби, крім цього сюди можна додати канали зв'язку, що поєднують конкретні маршрутизатори, комутатори та сервери.

Послуги, що надаються клієнтам, надаються в якості транспортних функцій та функцій включення до служб, що гарантують доступ до інформаційно-телекомунікаційної мережі, інших служб, наприклад телефонної служби, служби перевірки якості сервісу, віртуальних приватних мереж, послуг швидкого пересилання повідомлень тощо. Оскільки постачальник послуг, а також його клієнти є потенційними суб'єктами загроз безпеки, то для їх захисту використовується рівень інформаційної безпеки послуги. Наприклад, зловмисники можуть спробувати заблокувати функції постачальника послуг або втрутитися в обслуговування окремих клієнтів.

РОЗДІЛ 2
СУЧАСНІ МЕТОДИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

2.1. Використання тестових інформаційно-технічних впливів для превентивного аудиту захищеності інформаційно-телекомунікаційних мереж

Мережа зв'язку спеціального призначення (МЗ СП) – мережа зв'язку, призначена для задоволення потреб органів державної влади, потреб оборони країни, безпеки держави та забезпечення правопорядку. Якщо намагатися сформулювати технічо, то поняття МЗ СП може бути описане наступним чином. Система зв'язку спеціального призначення (СЗ СП) – це комплекс розділених у просторі взаємозв'язаних між собою технічних засобів та обслуговуючого персоналу, що виконують завдання щодо забезпечення обміну деякою інформацією в мережах військового та державного управління, а також у системах управління забезпеченням безпеки та правопорядку [7, с. 41].

Аналіз структури СЗ СП та принципів її функціонування, представлених у роботах, показав, що СЗ СП є складною організаційно-технічною системою (ОТС), що складається із сукупності різнорідних ІТКС спеціального призначення (ІТКС СП). При цьому під ІТКС СП розумітимемо таке [8, с. 4].

Інформаційно-телекомунікаційна мережа (ІТКМ) – це сукупність пов'язаних лініями зв'язку мережевих вузлів, що заснована на єдиній транспортній технології та експлуатується відповідно до єдиних принципів маршрутизації, адресації та управління, при цьому у її складі є граничні вузли, відповідальні за допуск інформації до мережі та направлення її до інших суміжні інформаційно-телекомунікаційні системи, а також вузли, відповідальні за формування, передачу, зберігання та обробку інформації. Узагальнюючи вищезгадане, зазначимо, що в даній статті як прототипу об'єкта КІ розглядається деяка абстрактна ІТКМ СП, як

складова частина СЗ СП, що у свою чергу входить до складу ЄСЕ України [7, с. 43-44].

Аналіз структури та принципів функціонування СЗ СП, проведений на основі робіт, показав, що на сучасному етапі свого розвитку СЗ СП зазнають ряду суттєвих змін. До основних таких змін відносяться:

- перехід від поєднання окремих СЗ СП у різних органах державного та військового управління до єдиної СЗ СП, заснованої на багатошелонованому принципі побудови (як правило СЗ СП включає до свого складу космічний, повітряний, наземний та морський ешелони);
- широка інтеграція до складу СЗ СП сегментів СС ОП та комерційних ІТКМ;
- активне заміщення в СЗ СП технологій комутації каналів на технології комутації пакетів;
- масове використання комерційних протоколів та технологій у складі СЗ СП, перш за все, протоколів IP (Internet Protocol) та MPLS (Multiprotocol label Switching);
- конвергенція окремих мереж та систем зв'язку в єдине інформаційне простір з урахуванням концепції NGN;
- широке використання супутникових систем зв'язку (ССЗ) як основи, що забезпечує глобальну зв'язність СЗ СП та глобальну керованість у всіх ланках державного управління, причому в склад СЗ СП можуть включатися ССЗ цивільних операторів супутникової зв'язку зі складу СЗ ВП;
- використання в мережах СЗ СП тактичної ланки технологій адаптивних мобільних радіомереж Mesh/MANET-мереж (Mobile Ad hoc Network);
- використання методів обробки «великих даних», а також хмарних та Grid-технологій для організації розподіленого зберігання та обробки великих масивів даних [8, с. 5].

При цьому для ІТКМ СП як «базового елемента» СЗ СП ці тенденції ведуть до наступної фундаментальної вразливості ІТКМ СП, яка суттєво знижує рівень її інформаційної безпеки (ІБ). Побудова ІТКМ СП на основі комерційних протоколів та технологій зв'язку, а також їх технологічна та інформаційна інтеграція з

комерційними ІТКС зі складу СЗ ВП, роблять можливим реалізацію інформаційно-технічних впливів (ІТВ) через СЗ ВП.

Питання забезпечення ІБ об'єктів КІІ є надзвичайно актуальними, що наголошується не лише у результатах наукових досліджень. Важливість проблематики ІБ об'єктів КІІ визнано в Україні на державному рівні, що спонукало з початку 2010-х років. розпочати роботи зі створення системи ДержСОПКА, яка забезпечила б аудит стану ІБ та захист об'єктів КІІ в Україні [7, с. 45-46].

Система ДержСОПКА заснована на централізованому використанні взаємопов'язаних між собою систем ідентифікуванняння втручань IDS (Intrusion Detection System), систем уникнення втручань IPS (Intrusion Prevention System), систем запобігання витоку конфіденційних даних DLP (Data Leak Prevention), а також систем управління інцидентами інформаційної безпеки SIEM (Security Information and Event Management). У складі ДержСОПКА створюється система державних та приватних центрів, що обслуговують суб'єкти КІІ. Такий центр бере на себе частину функцій безпеки, необхідних для протидії ІТБ на ІС суб'єктів КІІ [8, с. 6].

Як правило, до таких функцій належить:

- виявлення та аналіз уразливостей, що обслуговуються ІС, координація дій щодо усунення виявлених уразливостей;
- аналіз подій, що реєструються компонентами обслуговуваних ІС, та засобів їх захисту для пошуку ознак ІТТ, спрямованих на ці системи;
- координація дій з реагування на виявлений ІТБ, а якщо атака призвела до інциденту – ліквідації наслідків такого інциденту;
- розслідування інцидентів та ретроспективний аналіз ІТБ, які не вдалося запобігти;
- інформування персоналу ІТТ, проведення кіберучень. Для виконання вищезазначених функцій, центри ДержСОПКУ тісно інтегруються з захищаються ІВ – вони отримують повні інвентаризаційні дані ІВ, контролюють їх захищеність та аналізують події, реєстровані їх засобами захисту.

При цьому ці центри не замінюють собою власні системи захисту ІВ, т.к. власники об'єктів КІІ мають забезпечувати їх ІБ самостійно, а центр ДержСОПКУ своєю діяльністю лише компенсує можливі помилки. Саме у такому вигляді концепцію системи ДержСОПКУ було затверджено Указом Президента України № До 1274 від 12.12.2014 р. «Про Концепцію ДержСОПКУ», а перші технічні рішення були випробувані в рамках пілотного проекту Міністерство економічного розвитку у 2016 р. У 2018 р. – сформовано головний центр, який відповідає за забезпечення ІБ КІІ в масштабі України, а також за взаємодія з іншими об'єктами КІІ – Національний координаційний центр з комп'ютерних інцидентів (НКЦКІ) [7, с. 47].

У роботі проведено аналіз ролі ДержСОПКА у нормативних документах про безпеку КІІ. Показано, що власники значних об'єктів КІІ зобов'язані виконувати вимоги ФСТЕК України щодо забезпечення безпеки цих об'єктів та створювати системи захисту цих об'єктів (ст. 10 ДЗ-187).

В відповідно до вимог ФСТЕК (Наказ ФСТЕК України від 25.12.2017 «Про затвердження Вимог щодо забезпечення безпеки значущих об'єктів критичної інформаційної інфраструктури України») у системі захисту повинні бути реалізовані базові заходи, багато з яких безпосередньо спрямовані на протидію ІТБ зловмисників [8, с. 7]:

- інвентаризація компонентів ІТКС та аналіз їх уразливостей;
- контроль та аналіз мережевого трафіку;
- моніторинг безпеки;
- антивірусний захист;
- запобігання вторгненням;
- реагування на інциденти тощо.

При цьому власник має право самостійно вирішувати, як саме будуть реалізовано ці заходи захисту. Більше того, ці заходи захисту є лише базовими, тобто необхідними, але не достатніми для забезпечення безпеки об'єкту КІІ. Відповідно до існуючих процедурами, власник об'єкту КІІ має самостійно провести аналіз загроз, актуальних для об'єкта, самостійно визначити, як мають бути реалізовані базові заходи захисту, і якщо їх виявиться недостатньо захисту від

загроз – самостійно посилити базові заходи захисту чи розробити додаткові. У таких умовах саме аудит ІБ є тим основним. інструментом, який дозволяє оцінити рівень загроз для об'єкта КІІ та рівень його захищеності [7, с. 48].

Аналіз цих робіт показує, що основними перспективними напрямками вдосконалення SEIM-систем аудиту об'єктів КІІ є:

- підвищення повноти та своєчасності збору даних про події у елементи та підсистеми ІТКС;
- підвищення інтелектуальності обробки даних про події в елементах та підсистемах ІТКС, у тому числі за рахунок використання технологій багатовимірного кореляційного аналізу та технологій штучного інтелекту;
- формування позитивного зворотного зв'язку в системі за рахунок своєчасного виявлення ІТТ та оперативного формування сценаріїв захисту від нього;
- моделювання дій зловмисників із автоматичною генерацією на основі результатів моделювання як високо-ймовірних сценаріїв дій зловмисників, так і адекватних та ефективних сценаріїв захисту;
- підвищення інтелектуальності людино-машинного інтерфейсу системи в частині адаптації візуалізації представлення інформації про події системі по відношенню до системи зорового сприйняття людини-оператора з метою підвищення інформативності та ергономічності системи [8, с. 8-9].

Водночас вищезазначені напрями підвищення ефективності SIEM-систем у складі центрів ДержСОПКА не усувають один з головних, На думку авторів, недоліків цих систем – центри ДержСОПКА за своїм принципом функціонування орієнтовані збір даних про вже інцидентах ІБ, що відбулися, а також на збір доказів для оперативного дослідження цих інцидентів.

Така орієнтованість центрів ДержСОПКУ на фіксування інцидентів у режимі «постфактум» обумовлена загальними недоліками існуючих підходів до аудиту стану ІБ ІВ. Проведений аналіз сучасних теоретичних підходів у галузі аудиту ІБ, представлений у роботах, показав, що завдання аудиту є перевірка та оцінювання ІТКС на відповідність критеріям, які визначають вимоги до рівня ІБ. [7, с. 49].

При цьому в даний час в теорії аудиту ІБ склалася ситуація, за якої більшість робіт у цій галузі орієнтоване на дослідження експертного аудиту та оцінки відповідності переважно на основі моделей аналізу ризиків, або на основі аналізу стандартів ІБ. При цьому, тестування та, особливо, тестування спеціальними ІТБ є недостатньо вивченою областю аудиту. Є окремі роботи, наприклад, які присвячені такому типу тестування «як тест на проникнення», проте дані роботи носять більшою ступеня практичний, ніж теоретичний характер.

Рисунок 2.1 - Основні етапи процесу тестування

Тестування – перевірка виконання вимог до системи за допомогою спостереження над її роботою у кінцевому наборі спеціально обраних ситуацій. Окремий захід щодо дослідження системи або спосіб вивчення процесів її функціонування називається тестом. Тестовий ІТВ – вплив на інформаційний ресурс, інформаційну систему, інформаційну інфраструктуру, на технічні засоби чи на програми, вирішальні завдання отримання, передачі, обробки, зберігання та відтворення інформації з метою виявити вразливість об'єкта на яке виробляється вплив [8, с. 10].

Загальна класифікація заходів, способів та засобів тестування, що використовуються при аудиті ІБ, представлена на рис. 2. В даний час склався підхід до тестування, коли переважна частина процесів оцінювання безпеки систем ґрунтується на аналізі відповідності формальним вимогам з ІБ або шляхом тестування на основі моделей. Разом з тим, вимоги щодо ІХ, як правило, формулюються за результати аналізу інцидентів, що призводить до того, що вони регулярно відстають від сучасних можливостей та практики дій зловмисників.

Роботи, присвячені питанням експериментального тестування реальних інформаційних систем, розглядають такі способи та сценарії виключно як «тестування на проникнення» або як «інструментальний аудит», при цьому проведення такого типу аудиту у вітчизняній практиці не регламентується якимось системним або хоча б загальнотеоретичним підходом.

У деяких вітчизняних роботах з тестування на проникнення акцент робиться на необхідності виявлення найбільш «видовищних» уразливостей чи тих уразливостей, усунення яких принесе максимальні економічні вигоди компанії, яка виконує аудит. Водночас, простежується тенденція до нарощування частки тестів, які проводяться у формі експериментальних досліджень реального об'єкту або його прототип. Особливо це характерно при тестуванні програмного забезпечення [7, с. 50-51].

Як правило, для цього використовуються віртуальні машини. яких здійснюється контрольоване виконання тестованого програмного забезпечення забезпечення. Подальший розвиток цього підходу до тестування призвело до розробки так званих кіберполігонів, які віртуалізують як апаратне, так і програмне забезпечення розподіленої інформаційної системи і дозволяють відпрацювати захист від різних відомих ІТБ. Зараз це напрямок активно розвивається і йому присвячені роботи [8, с. 11].

2.2. Оцінка живучості розподілених інформаційно-телекомунікаційних мереж

Маршрутизація пакетів повідомлень в ІТКС та передача їх по лініях зв'язку для забезпечення інформаційного обміну між кореспондентами здійснюється у транзитних вузлах СЗЗК. Визначення маршруту руху пакетів повідомлень до СЗЗК є складним завданням, так як між кожною парою кореспондентів існує великий асортимент альтернативних маршрутів. Вибір маршруту здійснюють у вузлах СЗЗК (маршрутизатор операторів зв'язку) [13, с. 31].

Критеріями вибору маршруту серед допустимих альтернатив є потенційна пропускна здатність і завантаженість ліній (каналів) зв'язку; затримки, що вносяться каналами, та їх надійність; кількість транзитних вузлів СЗЗК та їхня надійність. Для забезпечення безпеки інформаційної взаємодії кореспондентів необхідно здійснювати порівняльну оцінку альтернативних структур ІТКС, що враховує здатність забезпечити інформаційну взаємодію кореспондентів в умовах навмисних та випадкових програмних перешкод, що призводять до зниження якості ІТКС та створюють нештатне навантаження на процеси пристрою, що реалізують інформаційну взаємодію.

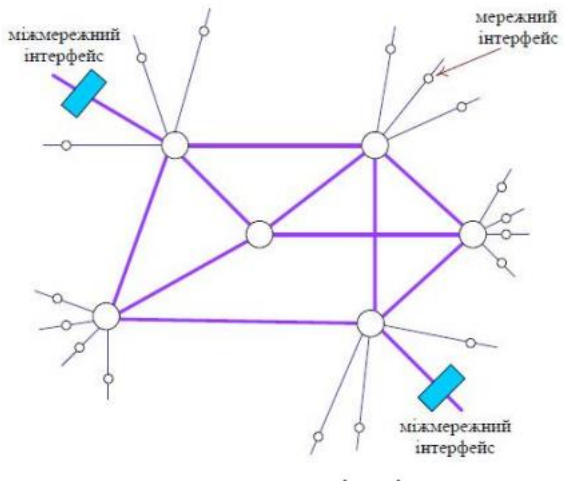

Рисунок 2.2 - Інформаційно-телекомунікаційна мережа

Така постановка завдання дозволяє сформулювати такі протиріччя. Протиріччя між необхідністю забезпечити високу достовірність результатів оцінки та збільшенням необхідного для її вирішення ресурсу, викликаного варіацією кількості ліній та вузлів зв'язку ІТКС, схильних до впливу перешкод. Протиріччя між потребою дати оцінку адаптаційним можливостям ІТКС та необхідністю отримання цієї оцінки перспективних значень показників безпеки вузлів та ліній зв'язку, що враховують деструктивну дію середовища [12, с. 19].

Методика спрямовано усунення зазначених протиріч. Інтегральним показником живучості ІТКС обрана ймовірність РНС порушення зв'язку між кореспондентами (абонентами), а показником живучості вузла ІТКС – коефіцієнт доступності КД і , де і = 1, 2, 3, …, n, що характеризує його можливості забезпечення абонентів послугами зв'язку з необхідною якістю. Порядок набуття значень показників, приватні критерії та їх внесок у підсумкову оцінку викладено нижче за тексту.

Теоретичною основою методики є теорії перколяції (від англ. percolation - протікання), математичної статистики та ймовірності. Вплив на ІТКС навмисних та випадкових програмних перешкод, що викликають послідовності відмов, аналогічно представленому в роботах процесу протікання (перколяції) та дає можливість описати глобально, але простий формі процеси епідемії на деградуючій структурі ІТКС. У рамках теорії перколяції така завдання вирішується по вузлам та зв'язкам [13, с. 31].

Модель деградації ІТКС, вирішення перколяційного завдання по вузлам Для досягнення мети методики під час вирішення перколяційного завдання по вузлам здійснюють наступну послідовність дій. Задають вихідні дані: схему зв'язку органів керування; вимоги до показників якості ІТКС та мінімальне допустиме значення комплексного показника безпеки ПКmin; ідентифікатори вузлів та наявність між ними ліній зв'язку. Структура та параметри розподіленої ІТКС (типологія її елементів) визначаються переліченими вихідними даними.

При цьому схема зв'язку та вимоги до показників якості ІТКС задає система вищого рівня ієрархії – система управління відомства, на користь якого організують

зв'язок. Якщо інформацію про структуру ССЗП неможливо отримати як вихідні дані від оператора зв'язку, то її попередньо знаходять моніторингом СЗЗК спеціалізованим ПЗ. Повнота та достовірність результатів моніторингу визначається кількістю та взаємною розташуванням (просторовим розмахом) засобів моніторингу [12, с. 20-21].

Достовірність у цьому випадку визначається ізоморфізмом результатів моніторингу та структури реальної СЗЗК. Доцільно мати пункти моніторингу у кожному захищеному сегменті ІТКС, підключеному до СЗЗК. Таке багатоагентне програмне забезпечення в результаті дозволить вирішувати завдання підсистеми моніторингу. топології та типології ІТКС для визначення всього асортименту альтернативних структур ІТКС для інформаційного обміну між органами управління.

Показник доступності (справної дії) і-го вузла ІТКС – коефіцієнт доступності, який обчислюють за формулою КД і = ((Ті -ТП і) / Ті) · 100%, де ТП і – тривалість інтервалу часу, протягом якого абонентам недоступні з необхідною якістю послуги від вузла зв'язку (час «простою»); Ті - сумарний час роботи вузла ІТКС. Вплив на вузол ІТКС випадкових та навмисних перешкод створює позаштатну (додаткове) навантаження на зв'язок та пристрої, її реалізують.

Як наслідок, ТП і – Тривалість інтервалу часу, протягом якого абонентам недоступні з необхідною якістю послуги від вузла зв'язку (час «простою») – збільшується, а показник доступності вузла ІТКС – зменшується. Досвід експлуатації ІТКС та експерименти на її Фрагменти показують, що значення мінімального допустимого значення показника доступності має бути задано в інтервалі 0,6 < КДmin < 1. [13, с. 32-33].

Далі необхідно визначити значення комплексного показника безпеки для кожного вузла ІТКС. Під комплексним показником і-го вузла ІТКС ПК і , розуміють згортку (її нормоване чисельне значення) параметрів безпеки, що характеризує здатність вузла ІТКС протистояти реалізації загроз безпеці. Розрахунок ПК і можна обчислити різними способами: підсумовуванням, або перемноженням, або як середнє арифметичне значення параметрів безпеки вузла [12, с. 22].

Крім цього попередньо задані вихідні дані як параметри ІТКС додатково задають мінімальне допустиме значення комплексного показника безпеки ПКmin для вузлів ІТКС та альтернативні варіанти підключення абонентів до ІТКС. Значення ПКmin задають як вимогу (тобто директивно) з урахуванням реалізації функцій безпеки, що забезпечують рівень мінімального довіри до виробника та експлуатанта обладнання (регламентується нормативно).

2.3. Програмно-апаратний захист інформації

2.3.1. Міжмережеві екрани

Перший компонент працює на пакетному рівні (рівні 3 та 4 моделі OSI). Його завдання полягає у виявленні підозрілих та некоректних пакетів, розпізнаванні сканування портів та прийнятті рішення про пропуск пакета у стек протоколу. Пакети можуть аналізуватися відповідно до таких критеріїв: формальна коректність пакета, напрямок пакета (вхідний або вихідний), хост та порт відправника, наявність встановлених прапорів [9, с. 7].

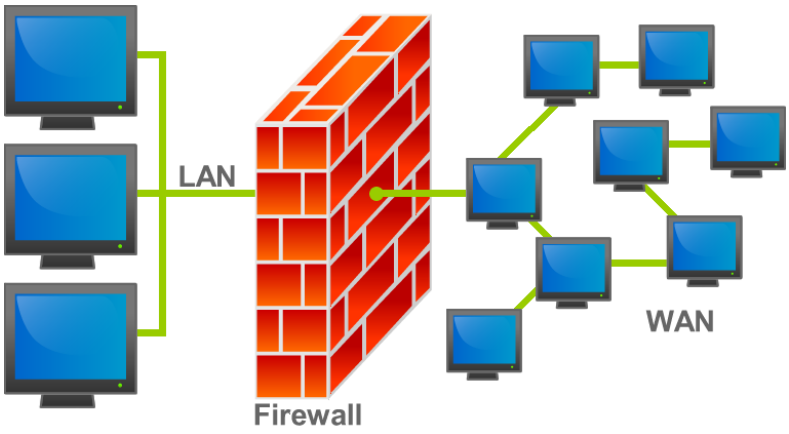

Рисунок 2.3 - Міжмережевий екран

Інший компонент МСЕ працює на вищому рівні, маючи справу з конкретними процесами. До його завдань входить визначення, чи можна дозволити процесу X

ініціювати з'єднання з цим хостом по даному порту, чи можна прослуховувати цей діапазон портів і т.д.

По суті, міжмережевий екран є сукупністю двох фільтрів – на рівні пакетів та на рівні процесів. Деталі реалізації змінюються від продукту до продукту, але функціональні принципи ядра дуже схожі. Серйозні програмні МСЕ використовують два драйвери для фільтрації на двох вищезгаданих рівнях. Також зазвичай є графічний інтерфейс, що дозволяє змінювати налаштування, але основна робота відбувається на рівні ядра, з використанням двох драйверів.

Що стосується нижчого рівня, пакетний фільтр зазвичай реалізується одним із двох способів. Перший спосіб базується на використанні драйвера NDIS (Network Driver Interface Specification). Цей драйвер знаходиться між драйвером мережної картки та драйверами. протоколів (TCP/IP тощо). По суті, це віртуальний адаптер, який є NIC драйвер для драйверів протоколу і навпаки.

Так як кожен вхідний та вихідний пакет проходить через цей проміжний драйвер, це дозволяє здійснити атаку «man-in-the-middle – людина посередині» (в даному випадку з доброю метою). Інший стандартний спосіб реалізації пакетного фільтра заснований на впровадженні в NDIS, шляхом перехоплення частини функцій бібліотеки NDIS, які використовуються драйверами протоколів. Це означає, що пакетний фільтр знаходиться в самому NDIS, між драйверами протоколів і чимось нижчим.

Незважаючи на те, що цей спосіб дуже сильно відрізняється від попереднього щодо реалізації, функціонально вони подібні. Тепер принцип роботи пакетного фільтра має бути зрозумілим. Він аналізує кожен пакет відповідно до критеріїв, вказаних у наборі правил МСЕ, збереженими в деякій внутрішній структурі даних. Здійснюється аналіз таких параметрів, як хост і порт відправника та одержувача, рівень фрагментації, тип протоколу, прапори пакета, чи пакет є частиною вже відкритого з'єднання і т.д.

Наприклад, якщо протокол – TCP, і пакет має SYN прапор (спроба відкрити з'єднання), фільтр в залежності від правил дозволить або заборонить з'єднання для даного вихідного та цільового хоста. Якщо все ж таки з'єднання буде дозволено,

фільтр додасть його до внутрішнього списку відкритих з'єднань. У такий спосіб міжмережевий екран слідкує за поточними з'єднаннями, здійснюючи безперервну інспекцію пакетів. Якщо пакет відповідає правилам або належить з'єднанню з вищезгаданого списку відкритих з'єднань, він пропускається [9, с. 8].

Пакетний фільтр передає пакет на наступний рівень – драйвера протоколів, якщо пакет вхідний, або драйвера мережної картки, якщо пакет вихідний. Якщо пакет блокується правилами, він ніколи не буде передано на наступний мережевий рівень. У цьому випадку опціонально, для зворотного зв'язку з користувачем, на екрані може з'явитися попередження та запис лог-файл.

Є також інші методи. Наприклад, WinSock API, набір функцій, що використовується більшістю програм для доступу до мережі, заснований на багаторівневій моделі, що дозволяє вставляти розширення (extensions) третіх осіб між інтерфейсом додатків та базовим мережевим протоколом.

Таке розширення можна додати, реалізувавши Layered Service Provider (LSP) і вставивши його в LSP-ланцюжок. LSP – це стандартна Windows DLL, що відповідає певній специфікації та має спеціальну функцію, яка призначається для вставки в ланцюжок WinSock протоколу. Згідно моделі WinSock, всі мережеві дані проходять через цей ланцюжок, в якому кожен LSP приймає рішення про пропуск даних на рівень вище (або нижче, залежно від того, чи є конкретні дані, що входять або вихідними), попередньо обробивши або змінивши дані відповідно до своєї функції [9, с. 9-10].

Quality of Service (QoS) є прикладом такого розширення, реалізованого як LSP. Фільтр процесів може бути реалізований у вигляді LSP, перебуваючи в ланцюжку протоколу і вибірково передаючи дані до наступного елемента ланцюжка або блокуючи їх, керуючись своїми умовами.

2.3.2. Віртуальні приватні мережі

Система захисту, що впроваджується, повинна забезпечити захист конфіденційного інформації, задовольняючи наступним вимогам [10, с. 88]:

1) лише зареєстровані користувачі можуть мати можливість входу в систему та обміну конфіденційною інформацією;

2) передана конфіденційна інформація має бути захищена криптографічними методами, що забезпечують її конфіденційність, цілісність та справжність;

3) з метою розслідування можливих інцидентів повинна вестись реєстрація в журналах найважливіших подій, пов'язаних з передачею інформації, що захищається канали зв'язку;

4) має бути забезпечена безпечна робота користувачів в Інтернеті засобами міжмережевого екранування.

Для виконання цих вимог використовувалася технологія VipNet. Програмний комплекс ViPNet складається з наступних компонентів: ПЗ ViPNet Administrator; ПЗ ViPNet Coordinator; ПЗ ViPNet Client. Технологія ViPNet забезпечує прозора взаємодія захищених комп'ютерів, незалежно від способу та місця підключення цих комп'ютерів до мережі, а також типу виділеної адреси.

При цьому забезпечується не лише гарантована захист трафіку, що передається між комп'ютерами, включеними до VPN, від перехоплення та модифікації шляхом його шифрування, але також захист самих комп'ютерів від мережевих атак з будь-якої точки мережі за рахунок інтегрованих в технологію ViPNet персональних та міжмережевих екранів. У мережі ViPNet використовується інтегрована багаторівневий захист від несанкціонованого доступу до мережі та до конфіденційної інформації.

Внаслідок створення системи захисту інформації на основі технології VipNet, були вирішені завдання з управління доступом користувачів до інформаційних ресурсів; забезпечено захист інформаційних ресурсів від усіляких мережевих атак з боку неконтрольованої мережі та захист переданих даних (захист від несанкціонованого доступу до інформації та забезпечення цілісності інформації чи захист від її спотворення) [10, с. 89-90].

Аналіз загроз інформаційної безпеки підприємства показав, що ризик інформаційної системи з використовуваною політикою безпеки становив 77,97%.

Ризик інформаційної системи після створення системи захисту та застосування необхідних контрзаходів із захисту інформаційних ресурсів становив 38,22%.

Висновки за розділом 2

Отже, з проведеного нами дослідження в другому розділі, можемо зробити такий висновок, що тестування – перевірка виконання вимог до системи за допомогою спостереження над її роботою у кінцевому наборі спеціально обраних ситуацій. Окремий захід щодо дослідження системи або спосіб вивчення процесів її функціонування називається тестом. Тестовий ІТВ – вплив на інформаційний ресурс, інформаційну систему, інформаційну інфраструктуру, на технічні засоби чи на програми, вирішальні завдання отримання, передачі, обробки, зберігання та відтворення інформації з метою виявити вразливість об'єкта на яке виробляється вплив

Модель деградації ІТКС, вирішення перколяційного завдання по вузлам для досягнення мети методики під час вирішення перколяційного завдання по вузлам здійснюють наступну послідовність дій. Задають вихідні дані: схему зв'язку органів керування; вимоги до показників якості ІТКС та мінімальне допустиме значення комплексного показника безпеки ПКmin; ідентифікатори вузлів та наявність між ними ліній зв'язку. Структура та параметри розподіленої ІТКС (типологія її елементів) визначаються переліченими вихідними даними.

Quality of Service (QoS) є прикладом такого розширення, реалізованого як LSP. Фільтр процесів може бути реалізований у вигляді LSP, перебуваючи в ланцюжку протоколу і вибірково передаючи дані до наступного елемента ланцюжка або блокуючи їх, керуючись своїми умовами.

РОЗДІЛ 3
ВЛАСНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ ЩОДО ОЦІНКИ ЗАХИЩЕНОСТІ МЕРЕЖ ТА ДЕЯКІ ПРИНЦИПИ І МЕТОДИ ЗАХИСТУ ІНФОРМЦАІЇ

3.1. Принципи інженерно-технічного захисту інформації телекомунікаційних мереж

Будь-яка технологія, зокрема захисту інформації, має відповідати набору певних загальних вимог, які можна охарактеризувати як загальні принципи захисту. До них відносяться:

- надійність захисту;
- неспинність захисту інформації;
- скритність захисту;
- цілеспрямованість захисту;
- раціональність захисту;
- активність захисту;
- гнучкість захисту інформації;
- різноманітність способів захисту;
- комплексне використання різних способів та засобів захисту інформації;
- економічність захисту інформації [11, с. 107-108].

Впевненість у захисті інформації можна мати лише тоді, коли точно гарантований потрібний рівень її захищеності, який не залежить від різних зовнішніх або внутрішніх чинників, що можуть мати вплив на безпеку інформації. При раціональному захисті на її рівень не повинні впливати навмисні дії зловмисника, наприклад вимикання електроживлення, так і стихійні сили, наприклад пожежа.

3.2. Методи захисту інформації технічними засобами

З метою уникнення витоку інформації формуються різноманітні методи (механізми), що застосовуються на усіх стадіях роботи з нею. Захищати від дефектів та зовнішніх впливів необхідно і прилади, на яких знаходиться важлива інформація, а також канали зв'язку. Дефекти можуть бути обумовлені несправністю обладнання або підробкою, або розголошенням. Пошкодження можуть бути спричинені поломкою обладнання, підробкою або розголошенням секретної інформації. Зовнішні дії з'являються як унаслідок стихійних нещасть, так і внаслідок збоїв обладнання чи крадіжки [14, с. 76].

Для збереження даних застосовують різноманітні методи захисту:

• безпека будівель, де знаходиться секретна інформація;

• контроль допуску до секретної інформації;

• розмежування доступу;

• дублювання каналів взаємозв'язку та приєднання резервних пристроїв;

• криптографічні перебудови інформації [22, с. 103];

Таким чином, небезпека захисту інформації здійснила засоби забезпечення інформаційної безпеки однієї з найважливіших характеристик інформаційної системи. Іншими словами, проблема захисту інформації та захисту інформації в інформаційних системах знаходять рішення з метою того, щоб сприяти ізолюванню функціонуючих інформаційних систем від несанкціонованих керуючих впливів та доступу сторонніх осіб або програм до даних із метою розкрадання. Інформація, будучи основним поняттям наукових напрямів, вивчає також процеси передачі, зберігання та переробки різної інформації. Інформація виникає у різних життєвих ситуаціях і потребує захисту. Інформаційну безпеку можна описати як гарну захищеність інформаційних ресурсів від випадкових або спеціальних природних чи штучних втручань, що загрожують заподіянням шкоди власникам або споживачам інформації.

Якщо говорити про мету інформаційної безпеки, то нею вважається захист даних системи, гарантія точності та цілісності даних, а також зменшення

руйнування за умов, якщо інформація стане зміненою або зовсім зруйнованою. На практиці важливими вважаються три вимоги інформаційної безпеки: Доступність – здатність за певне час придбати необхідну інформаційну послугу [14, с. 77-78]. Цілісність – її безпека від руйнування та несанкціонованої зміни. Конфіденційність – захист від несанкціонованого прочитання. Саме доступність, цілісність та конфіденційність є рівнозначними складовими. інформаційної безпеки. Методи захисту інформації. Під фразою «загрози безпеки інформаційних систем» розуміються справжні або потенційно можливі дії чи події, готові змінити збережені в інформаційній системі дані, сприяти їх знищенню або застосовувати в будь-яких інших цілях, не передбачених регламентом попередньо. Передбачення потенційних загроз безпеці інформації проводиться для того, щоб визначити повний комплекс вимог до системи, що розробляється для забезпечення захисту інформаційних ресурсів [22, с. 104-105].

Необхідність класифікації загроз безпеці інформаційної системи обумовлена тим, що інформація, що зберігається, схильна впливу надзвичайно широкого числа факторів, що веде до складності формалізувати проблему опису повної множини загроз. Тому прийнято визначати не повний перелік загроз, а класифікацію.

Для того, щоб класифікувати загрози було використано підхід, який запропонував Стів Кент. Дана класифікація не втрачає актуальності і на сьогоднішній день і являє собою основу для більшості описів загроз захисту. Розглянемо види умисних загроз безпеки інформації, їх поділяють на: пасивні загрози орієнтовані переважно на несанкціоноване застосування інформаційних ресурсів ІС, але при цьому не впливаючи на діяльність системи. Як приклад можна привести незаконний доступ до баз даних або ж прослуховування різних каналів для зв'язку [14, с. 79-80].

Активні загрози майже завжди мають за ціль недотримання стандартної діяльності ІС у вигляді спрямованого впливу її елементи. До активних загроз належать, наприклад, псування професійного комп’ютера або його окремих частин, зміна відомостей, руйнування програмного забезпечення комп'ютерів, недотримання роботи ліній зв'язку та і т.д. Основою активних загроз зазвичай є прямі дії

злочинців, шкідливі програмні забезпечення і подібне. Крім того, навмисні загрози діляться на внутрішні, що виникають всередині керованої організації, і зовнішні [22, с. 106].

3.3. Власні висновки та рекомендації щодо оцінювання захищеності мереж

На основі проведеного дослідження було сформовано власні висновки та рекомендації щодо оцінювання захищеності інформаційно-телекомунікаційних мереж :

необхідно захищати від дефектів та зовнішніх впливів і прилади, на яких знаходиться важлива інформація, і також канали зв'язку;

важливо приділити достатню увагу захисту від підключення сторонніх технічних каналів витоку;

можна убезпечити зв'язок від індуктивних наведень та запобігти витоку інформації, що охороняється за допомогою генераторів шуму. Пристрій можна використовувати в телефоні, він зашумляє телефонні лінії, які були спільно прокладені, у всіх діапазонах звукових частот;

проблема тестування та оцінки засобів забезпечення інформаційної безпеки, оцінки захищеності автоматизованих систем є на сьогоднішній день актуальною, що підтверджується аналізом вітчизняних та зарубіжних стандартів у цій галузі. Важливим елементом оцінки стану безпеки є тестування як підтвердження того, що засоби захисту відповідають стандартам та функціонують коректно;

необхідно завжди уважно визначати маршрут руху пакетів повідомлень до СЗЗК, так як між кожною парою кореспондентів існує великий асортимент альтернативних маршрутів. Критеріями вибору маршруту серед допустимих альтернатив є потенційна пропускна здатність і завантаженість ліній (каналів) зв'язку; затримки, що вносяться каналами, та їх надійність; кількість транзитних вузлів СЗЗК та їхня надійність;

стандарти з оцінки безпеки практично не містять конкретних методик, внаслідок чого величина розриву між загальними деклараціями та конкретним

інструментарієм щодо реалізації та контролю їх положень є неприпустимою. Внаслідок аналізу даних стандартів можна зробити висновок, що їхнє успішне застосування вимагає розробки додаткових спеціальних методів, алгоритмів та методик оцінювання захищеності та проведення процесу тестування.

Висновки за розділом 3

Отже, на основі проведеного нами дослідження в даному (третьому) розділі, попередньо проаналізувавши весь вище викладений матеріал, ми можемо зробити наступні висновки:

Нами було визначено, що з метою уникнення витоку інформації формуються різноманітні методи (механізми), що застосовуються усім стадіях роботи з нею. Дефекти можуть бути обумовлені несправністю обладнання або підробкою, або розголошенням Пошкодження можуть бути спричинені поломкою обладнання, підробкою або розголошенням секретної інформації. Зовнішні дії з'являються як унаслідок стихійних нещасть, так і внаслідок збоїв обладнання чи крадіжки.

Існують прилади, які роблять аналіз телефонної лінії завдяки застосуванню нелінійної локації, але вони не використовуються в широких масах через складність налаштування та отримання неоднозначних результатів. Важливо приділити достатню увагу захисту від підключення сторонніх технічних каналів витоку.

Можна убезпечити зв'язок від індуктивних наведень та запобігти витоку інформації, що охороняється за допомогою генераторів шуму. Пристрій можна використовувати в телефоні, воно зашумляє телефонні лінії, які були спільно прокладені, у всіх діапазонах звукових частот.

ВИСНОВКИ

Отже, на основі проведеного нами дослідження в даній дипломній роботі, попередньо проаналізувавши весь вище викладений матеріал, ми можемо зробити наступні висновки:

1. Інформаційна безпека заснована на багатошарових принципах безпеки. Це означає, що безпека гарантується на кожному рівні моделі ВВС, а відповідні функціональні послуги розподіляються між цими рівнями. Служби безпеки поділяються на фазу зв'язку та рівень ВВС. Існують відмінності в застосуванні однієї і тієї ж послуги на різних рівнях. За запитом певні послуги безпеки не потрібні. Конкретні послуги надаються на кількох рівнях.

2. Загрози інформаційній (комп’ютерній) безпеці – це різноманітні дії, які можуть призвести до порушення інформаційної безпеки. Іншими словами, це потенційні події, процеси чи дії, які можуть пошкодити інформацію та комп’ютерні системи. Загрози інформаційної безпеки можна розділити на дві категорії: природні загрози та техногенні загрози. До природних явищ належать ті, які залежать від людини, наприклад, урагани, повені, пожежі тощо.

3. Проблема тестування та оцінки засобів забезпечення інформаційної безпеки (ІБ), оцінки захищеності автоматизованих систем (АС) є на сьогоднішній день актуальною, що підтверджується аналізом вітчизняних та зарубіжних стандартів у цій галузі. Важливим елементом оцінки стану безпеки є тестування як підтвердження того, що засоби захисту відповідають стандартам та функціонують коректно.

4. Мережа зв'язку спеціального призначення (МЗ СП) – мережа зв'язку, призначена для задоволення потреб органів державної влади, потреб оборони країни, безпеки держави та забезпечення правопорядку. При цьому, технічно поняття МЗ СП може бути наступним чином.

5. Маршрутизація пакетів повідомлень в ІТКС та передача їх по лініях зв'язку для забезпечення інформаційного обміну між кореспондентами здійснюється у

транзитних вузлах СЗЗК. Визначення маршруту руху пакетів повідомлень до СЗЗК є складним завданням, так як між кожною парою кореспондентів існує великий асортимент альтернативних маршрутів. Вибір маршруту здійснюють у вузлах СЗЗК (маршрутизатор операторів зв'язку).

6. Наприклад, WinSock API, набір функцій, що використовується більшістю програм для доступу до мережі, заснований на багаторівневій моделі, що дозволяє вставляти розширення (extensions) третіх осіб між інтерфейсом додатків та базовим мережевим протоколом.

7. Внаслідок створення системи захисту інформації на основі технології VipNet, були вирішені завдання з управління доступом користувачів до інформаційних ресурсів; забезпечено захист інформаційних ресурсів від усіляких мережевих атак з боку неконтрольованої мережі та захист переданих даних (захист від несанкціонованого доступу до інформації та забезпечення цілісності інформації чи захист від її спотворення).

8. З метою уникнення витоку інформації формуються різноманітні методи (механізми), що застосовуються усім стадіях роботи з нею. Захищати від дефектів та зовнішніх впливів необхідно і прилади, на яких знаходиться важлива інформація, а також канали зв'язку. Дефекти можуть бути обумовлені несправністю обладнання або підробкою, або розголошенням Пошкодження можуть бути спричинені поломкою обладнання, підробкою або розголошенням секретної інформації. Зовнішні дії з'являються як унаслідок стихійних нещасть, так і внаслідок збоїв обладнання чи крадіжки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ємельянов С.Л. Основи інформаційної безпеки. Одеса: Фенікс, 2014. 357 с.

2. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. К.: ВД “Гельветика”, 2017. 168 с.

3. Остапов С. Е. Технології захисту інформації: навч. посіб. Харків, 2013. 476 с. 8 Електронне урядування: опорний конспект лекцій. К., 2012. 264 с.

4. Громико І. О. Загальна парадигма захисту інформації: визначення термінів від носіїв до каналів витоку інформації / І. О. Громико // Системи обробки інформації. Х.: ХУПС, 2016. Вип. 9 (58). С. 3-9.

5. Кобозева А.А. Аналіз захищеності інформаційних систем: підручник / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. К.: ДУІКТ, 2010. 316 с.

6. 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, 2019, 300 с.

7. Новицький А. Правове регулювання інституціоналізації інформаційного суспільства в Україні : [монографія] / А. Новицький. – Ірпінь : НУ ДПС України, 2011. 444 с.

8. Гуцалюк М.В., Гайсенюк Н.А. Організація захисту інформації. – К.: Альтерпрес, 2015. 541 с.

9. Марущак А.І. Технологічні основи захисту інформації з обмеженим доступом: курс лекцій. – К.: КНТ, 2017. 208 с.

10. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації / В. Василюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 2 (13). – С. 88–102.

11. Клімушин П.С. Електронне урядування в інформаційному суспільстві: монографія / П.С. Клімушин, А.О. Серенок. – Х.: Вид-во ХарРІ НАДУ «Магістр», 2010. 312 с.

12. Богуш В.М. Криптографічні застосування елементарної теорії чисел / В.М. Богуш, В.А. Мухачов. – К.: ДУІКТ, 2016. 126 с.

13. Головань С. Про термінологію в області безпеки інформації / С. Головань, А. Давиденко, Л. Щербак // Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова. – 2013. Вип. 66. С. 31–35.

14. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. … канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / О. Шепета ; Нац. академія Служби безпеки України. – К., 2011. 215 с.

15. Андрєєв В.І. Основи інформаційної безпеки: підручник / В.І. Андрєєв, В.О. Хорошко, В.С. Чередніченко [та ін.] – К.: ДУІКТ, 2019. 292 с.

16. Задорожня Л. М., Коваль М. І., Брижко В. М. Питання вдосконалення законодавства України у сфері інформації та інформатизації: додаток до наукового журналу “Правова інформатика”. / За ред. чл.-кор. АПрН України М. Я. Швеця. – К.: НДЦПІ, 2015. 31 с.

17. Закон України «Про захист інформації в автоматизованих системах» // *Відомості Верховної Ради України*, 1994. № 31. С. 286.

18. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики. – К.: АДПС України, 2018. 187 с.

19. Казакова Н.Ф. Задачі захисту інформаційних ресурсів від впливу зовнішніх загроз // Матер. II молод. наук. конф. «Сучасні інформаційні технології в повсякденній діяльності та підготовці фахівців», 31 березня 2016 р., Одеса : ОНЮА, 2016. 69 с.

20. Казакова Н.Ф. Інформаційне забезпечення системи управління якістю продукції в сфері телекомунікацій // Тр. IV Междунар. научнопракт. конф. «Системы и средства передачи и обработки информации»: ОАО «Нептун», УГАС им.А.С.Попова, Одесса, 6-14 сент. 2010 г. Одесса, 2020. С. 59-61.

21. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть [Текст] / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. 2019. № 14 : Міжнародні відносини. С. 46-48.

22. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. 288 с.

23. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. / Б.А. Кормич. К., Принт. 2014. 169 с.

24. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: "Кондор", 2014. 384.

25. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навч.-метод. посіб. / А. Б. Кочарян, Н. І. Гущина. К., 2019. 100 с.

26. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. Х.: Вид. ХНЕУ, 2018. 510 с.

27. Ляшенко І. О. Європейські критерії безпеки інформаційних технологій. Сучасні інформаційні технології у сфері безпеки та оборони. 2012. № 1 (13). С. 84–86.

28. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, С.Б. Гордієнко, О.С. Петров, В.О. Хорошко, Л.М. Щербак; під ред. В.О. Хорошко. – Луганськ: Ноулідж, 2012. 480 с.

29. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. Х.: УВС, 2020. 368 с.

30. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22; 22. НД ТЗІ 2.5-008-2002.

31. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2019. С. 22.

32. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

33. Бабаєв В.М. Електронне урядування: текст лекцій / В.М. Бабаєв, М.М. Новікова, С.О. Гайдученко. Х.: ХНУМГ, 2014. 127 с.

34. Постанова Кабінету Міністрів України “Про створення Національного автоматизованого інформаційного фонду стандартів” від 01.02.1995 р. № 84 із змінами, внесеними Постановою КМУ від 16.03.2000 р. № 501.

35. Правова інформатика: системна інформатизація законотворчої, правозастосовної, правоохоронної, судочинної та правоосвітньої діяльності в Україні. – Ужгород: ІВА, 2020. 611 с.

36. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2017. 365 с.

37. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – К. : Держстандарт України, 2017. 15 с.

38. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. – К. : Держстандарт України, 2017. 16 с.

39. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

40. Цимбалюк В. С. Окремі питання щодо визначення категорії “інформаційна безпека” у нормативно-правовому аспекті. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2014. № 8.С. 30-33.

41. Цимбалюк В. С. Сутність і зміст правової інформатики (методологічний аспект). // Правова інформатика. – 2005. – № 4(8). – С. 18-30.

42. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє. В. М. Фурашев, Д. В. Ланде, О. М. Григор’єв, О. В. Фурашев. – К.: Інжиніринг, 2015. 164 с.

43. Якубівська Ю. Є. Колізії норм права та компетенції органів управління у сфері інтелектуальної власності як загроза інформаційній безпеці / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Юридичні науки. - К. : УДУФМТ, 2015. № 4 (81). С. 37-42.