Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження і обгрунтування вибору методів інформаційної безпеки ІТ компанії
(тема)

Виконав:
студент 2 курсу, групи АМСЗІм-18-1
Тертичний В.О.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: професор кафедри ІКІ ім. В.В. Поповського
Шостко І.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2020 р .

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студенту Тертичному Владиславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження і обгрунтування вибору методів інформаційної безпеки IT компанії затверджена наказом по університету від «17» березня 2020 р. №465 Ст.

2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020 р.

3. Вихідні дані до роботи: загальна методика оцінки ризиків CVSS, закон України про інформацію, міжнародний стандарт NIST SP 800-84, міжнародний стандарт NIST SP 800-53

4. Перелік питань, що потрібно опрацювати в роботі:

1) Аналіз існуючих загроз для інформаційних систем
2) Визначення імовірності порушення критичних властивостей інформаційного активу на основ CVSS
3) Обгрунтування підходів до впровадження технічних рішень в систему інформаційної безпеки компанії
4) Моделювання системи інформаційної безпеки в IT-компанії

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Шостко Ігор Святославович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.03.2020	Виконано
2	Збір матеріалів для дослідження	28.03.2020	Виконано
3	Розробка 1 розділу	01.04.2020	Виконано
4	Розробка 2 розділу	10.04.2020	Виконано
5	Розробка 3 розділу	19.04.2020	Виконано
6	Розробка 4 розділу	29.04.2020	Виконано
7	Розробка 5 розділу	05.05.2020	Виконано
8	Оформлення атестаційної роботи	10.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студент _____ Тертичний В.О.
(підпис) (прізвище, ініціали)

Керівник роботи _____ професор Шостко І.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 7 рис., 8 таблиць, 14 джерел.

CVSS, ІМОВІРНІСТЬ, КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ, ІНЦИДЕНТ, КОНФІДЕНЦІЙНІСТЬ, ДОСТУПНІСТЬ, ЦІЛІСНІСТЬ.

Об’єкт дослідження – процес створення комплесної системи захисту корпоративної мережі.

Предмет дослідження – методи і засоби захисту корпоративних мереж.

Мета роботи – аналіз шляхів впровадженя або підвищення ефективності побудови сучасних систем захисту корпоративних мереж.

Методи досліджень – емпіричний аналіз, формалізація та порівняння.

У роботі виконаний аналіз поточного стану засобів захисту інформації в мережах. Розглянуті їх переваги та недоліки. Також були розглянуті основні типи атак на мережі, з цілью розуміння принципів їх дії, для побудови якісної системи захисту мереж. Також в роботі був використаний математичний апарат теорії імовірності для визначення порушення критичних властивостей інформаційного активу на основі CVSS.

ABSTRACT

The report contains: 81 p., 7 fig., 8 tables, 14 sources.

CVSS, PROBABILITY, CORPORATE NETWORK, PROTECTION, INCIDENT, CONFIDENTIALITY, ACCESSIBILITY, INTEGRITY.

The object of research is the process of creating a comprehensive system of corporate network protection.

The subject of research – methods and means of protection of corporate networks.

The purpose of the work – analysis of ways to implement or increase the efficiency of modern systems of protection of corporate networks.

Research methods – empirical analysis, formalization and comparison.

The analysis of the current state of information security in networks is performed in the work. Their advantages and disadvantages are considered. The main types of attacks on the network were also considered, in order to understand the principles of their operation, to build a quality system of network protection. The mathematical apparatus of probability theory was also used to determine the violation of the critical properties of the information asset based on CVSS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ІА – інформаційний актив
ІКСМ – інформаційно-комунікаційні системи та мережі
ІС – інформаційна система
МЕ – міжмережевий екран
ОС – операційна система
ПЗ – програмне забезпечення
ТЗ – технічні заходи
CERT – computer emergency response team
CVE – common vulnerabilities and exposure
CVSS – commom vulnerability scoring system
DDOS – disturbed denial of service
DES – data encryption standart
DOS – denial of service
DNS – domain name system
EIP – extended instruction pointer
ESP – extended stack pointer
ICMP – internet control message protocol
IDS – intrusion detection system
IDMEF – intrusion detection message exchange format
IPS – intrusion protection system
NGFW – next generation firewall
PAM – privilege access management
PPP – point to point protocol
RAM – random access memory
ROM – read only memory
SMB – small medium bussines
VPN – virtual private network
VTP – vlan trunkling protocol

ВСТУП

У міру зростання обсягів даних, з якими оперують користувачі інформаційних систем, зростають труднощі успішного ведення бізнесу. Однією з найважливіших завдань для успішного функціонування інформаційної системи підприємства є забезпечення збереження даних в мережі. Так як цифрові дані є основою організацій, то безпека даних – це основа грамотного ведення бізнесу.

Наслідки комп'ютерних збоїв відображаються не лише на працівниках компаній та адміністраторах мереж, а також, з мірою розвитку платежів та безпаперового документообігу, на функціонуванні великих банківських систем та великих корпорацій, що безумовно приведе до збитків.

Тому захист даних в комп'ютерних мережах стає однією з найгостріших проблем.

З урахуванням всіх обставин приймаються рішення про розробку та реалізацію комплексних проектів на базі широкого спектра систем і рішень, поєднання яких дозволяє забезпечити ефективний захист інформаційних ресурсів корпоративної мережі.

Для збереження конфіденційних даних в середині компанії потрібно побудувати систему захисту інформації. Однак при її побудові потрібно зберегти принципи конфіденційності, цільності та доступності. Однак побудова системи інформаційної безпеки неможлива без ідентифікації та оцінки ризиків.

Хоча міжнародний стандарт ISO 27000 не дає яку саме методику оцінки ризиків використовувати, зазвичай ця задача покладається на керівників підприємств, або відповідального за створення системи інформаційного захисту на підприємстві.

Метою роботи є розробка системи захисту в IT-компанії та визначення імовірності порушення критичних властивостей інформаційного активів компанії на основі методики Common Vulnerability Scoring system (CVSS).

Для вирішення даної мети були поставлені наступні задачі. По перше проаналізувати та класифікувати основні види загроз в комп'ютерних мережах, по друге дослідити методику загальної оцінки враливостей CVSS. Також необхідно дослідити методи захисту комп'ютерних мереж та надати рекомендації щодо їх впровадження в комп'ютерну мережу IT компанії. Крім того потрібно описати

підхід до проектування системи безпеки, а також необхідно описати план дій при інцидентах інформаційної безпеки. У тому числі потрібно описати та обгрунтувати засоби безпеки для змодельованої мережі.

Для вирішення поставлених задач, в першому розділі атестаційної роботи були описані та класифіковані основні види загроз для мереж та описані структури мережі та особливості їх планування, зокрема для IT компаній.

У другому розділі було описано класифікація інформації в компанії, також була описана загальна система оцінки вразливостей CVSS.

В третьому розділі були розглянута загальна класифікація засобів захисту мереж та більш детально розглянуті засоби технічного захисту. Також були надані технічні рекомендації щодо побудови захищеної мережі компанії.

Четвертий розділ описує поетапний підхід до проектування системи інформаційної безпеки, також був запропонований підхід щодо дії при інцидентах інформаційної безпеки.

В п’ятому розділі були запропоновані технічні рішення для побудови системи захисту на підприємстві. На основі математичного апарату теорії ймовірностей, були пораховані ймовірності компроментації критичних вузлів компанії до впровадження захисту та після. Було проведено порівняльний аналіз результатів та на їх основі зроблені висновки.

1 СТРУКТУРА МЕРЕЖІ ІТ КОМПАНІЙ ТА ОСНОВНІ ВИДИ ЗАГРОЗ

Локальна мережа дозволяє знаходити, обробляти і передавати всі внутрішні дані компанії максимально оперативно, що важливо для коректної роботи підприємства. Крім того, за допомогою спеціального обладнання і програмного забезпечення можна налагоджувати партнерські відносини з потенційними клієнтами, виконавцями завдань і іншими учасниками бізнес-процесу.

Доступ до загальної інформації про фірму або компанії дається не тільки певної групи користувачів шляхом привласнення унікального пароля, але і всім бажаючим через відображення основних даних в мережі Інтернет.

1.1 Структура локальної мережі підприємства

Висока популярність мережі Інтернет та стрімкий розвиток інформаційних технологій призвело до того, що всі компанії, незалежно від виду діяльності, будують локальні мережі для вдосконалення системи передачі та обробки даних як всередині підприємства, так і для оперативної комунікації з потенційними партнерами або замовниками ззовні. За допомогою такого інтерактивного і простого способу взаємодії можна досягти високих результатів в побудові успішної ІТ компанії [1].

Основні складові локальної мережі підприємства:

- мережеві адаптери;
- концентратори;
- програмне забезпечення;
- комутатори;
- маршрутизатор;
- кабельна система.

Складна і розвинена структура локальної мережі підприємства складається з багатьох компонентів, які забезпечують її коректну роботу. Щоб всі елементи мережі працювали безперебійно і давали можливість працівникам швидко отримувати дані та обробляти їх, потрібно грамотно планувати прокладку і установку устаткування і з'єднання всіх елементів. Тільки чітко структурована система, що відповідає всім потребам підприємства, дасть можливість здійснювати всі операції.

1.2 Ієрархія корпоративних мереж

Ієрархічна структура мереж компаній являє собою складний механізм, що складається з декількох шарів, які постійно взаємодіють між собою.

Всю систему можна представити у вигляді піраміди, складові якої розташовуються знизу вгору таким чином [1].

1) Комп'ютери, в яких зберігається і обробляється інформація, і транспортна підсистема, за допомогою якої можна швидко пакетний канал доступу між комп'ютерами.

2) Шар мережних операційних систем, розташований над транспортною системою. Він відповідає за коректну роботу додатків в комп'ютерах і доставляє через транспортну систему в спільне користування ресурси свого комп'ютера.

3) Окремим шаром корпоративної мережі є системні програми, які керують базами даних, зберігають їх у впорядкованому вигляді і дозволяють проводити з ними різні операції.

4) Наступним рівнем системи є системні сервіси, які використовують системи управління базами даних для пошуку інформації та надання її користувачам в зручному вигляді. До складу цих систем входить Інтернет, електронна пошта та інші корпоративні інструменти.

5) На останньому рівні піраміди розташовані специфічні системи, які виконують спеціальні завдання, необхідні для підприємства. До таких завдань можна віднести автоматизацію банківських систем, автоматизацію різних процесів і подібні операції.

1.3 Особливості планування структури мережі підприємства

Забезпечення надійного захисту корпоративної мережі – дуже складний процес, який являє собою безперервну і постійну послідовність дій по реалізації комплексу заходів інформаційної безпеки.

При прийомі співробітника на роботу слід враховувати, що фахівець з безпеки інформації відповідає за розробку, реалізацію та експлуатацію системи забезпечення інформаційної безпеки, спрямованої на підтримку цілісності, придатності та конфіденційності даних, накопичених в компанії. У його функції входить забезпечення і фізичної (технічні засоби, лінії зв'язку і віддалені

комп'ютери), і логічної (самі дані, прикладні програми, операційна система) захисту інформаційних ресурсів.

Складність створення системи захисту інформації обумовлена тим, що дані можуть бути викрадені з комп'ютера, одночасно залишаючись на місці. До того ж цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні. При забезпеченні безпеки інформації необхідно приймати не тільки витрати на закупівлю і установку різних технічних або програмних засобів, але і питання кваліфікованого визначення розумних меж безпеки і відповідного підтримки системи в працездатному стані. Об'єктами посягань можуть бути як самі матеріальні технічні засоби (комп'ютери і периферія), так і програмне забезпечення і бази даних [1].

Головним завданням, розв'язуваної на етапі проектування підсистеми інформаційної безпеки, є забезпечення безпеки інформації в комп'ютерних мережах, що передбачає створення перешкод для будь-яких несанкціонованих спроб розкрадання або модифікації даних, що передаються в мережі. У той же час дуже важливо зберегти такі властивості інформації, як доступність, цілісність і конфіденційність. Доступність інформації має на увазі забезпечення своєчасного і безперешкодного доступу користувачів до потрібних відомостей. Цілісність інформації полягає в її існуванні в неспотвореному вигляді, тобто незмінному по відношенню до деякого фіксованого її стану. Конфіденційність передбачає необхідність введення обмежень доступу до даної інформації для певного кола користувачів.

Перш ніж приступити до створення підсистеми інформаційної безпеки мережі, необхідно розробити концепції і політики безпеки, які будуть прийняті в компанії і які нерозривно пов'язані із загальним планом її розвитку. Правильна політика безпеки дозволить не тільки врахувати всі вимоги з безпеки, а й оптимально використовувати фінансові кошти, необхідні для її реалізації. У політиці безпеки повинні бути враховані всі складові інформаційної безпеки. В першу чергу потрібно визначити список об'єктів, на які можуть бути спрямовані загрози. Тому, всі критично важливі вузли корпоративної мережі, повинні бути додані в цей список.

Необхідно провести аудит і аналіз існуючих і можливих зовнішніх і внутрішніх загроз, визначити їх джерела і оцінити ризики. Ці відомості дозволять

скласти реальне уявлення про існуючу і прогнозованою ступеня уразливості корпоративної мережі, а також про потреби в захисті інформаційних ресурсів.

За результатами проведеного аналізу можливих загроз визначаються методи і засоби виявлення ворожого впливу і захисту від відомих загроз, а також методи і засоби реагування при інцидентах. Необхідно пам'ятати, що збиток часто наноситься не через чийогось злого наміру, а просто через елементарних помилок користувачів, які випадково псують чи видаляють дані, вкрай важливі для компанії.

1.4 Основні типи загроз для корпоративних мереж

Проблема захищених ресурсів інформаційно-комунікаційних систем та мереж (ІКСМ), є ще більш актуальною у зв'язку з розвитком та розподілом глобальних мереж, територіально розподілених інформаційних комплексів та систем з удаленим управлінням доступом до інформаційного ресурсу.

Відомий аргумент для підвищення уваги до питань безпеки ІКСМ являє собою бурхливу розробку програмно-апаратних методів для захисту звичайного користувача системи від несакціонованих дій зловмисника та збереження критичних властивостей інформації (конфіденційності, доступності, цілісності).

Серед загроз для SMB можна виділити [2].

1) Крадіжка конфіденційної інформації – тип атаки, при якій зловмисник або незадоволений працівник крадуть інформацію, яка є важливою для компанії.

2) Дефейс сайту – тип атаки, при якій сторінка web-сайту замінюється іншою сторінкою, найчастіше містить рекламу, загрози або викликають попередження.

3) Фішинг – тип атаки, при якій зловмисник отримує важливу інформацію (наприклад, логіни, паролі або дані кредитних карт) шляхом підроблення повідомлень від довіреного джерела (наприклад, електронний лист, складене як законне, обманом змушує одержувача натиснути на посилання в листі, яка встановлює шкідливе програмне забезпечення на комп'ютер).

4) Програма-вимагач – тип шкідливого програмного забезпечення, що блокує доступ до даних на комп'ютері, в результаті чого злочинці вимагають викуп за те, щоб розблокувати заблоковані дані.

5) Втрата даних через природних явищ або нещасних випадків.

Однак потрібно пам’ятати, що неможливо розробити спеціальні програмно-апаратні засоби захисту від всіх загроз оскільки з кожним днем їх кількість та різноматність стрімко збільшується.

Указаний вплив може бути реалізований технічно або організаційно, тільки в тому випадку, коли відома інформація про принципи роботи ІКСМ, її структуру, програмне забезпечення та інші [2].

1.5 Класифікація атак на мережу та засоби їх протидії

В даний час існує декілька класичних визначень поняття атака на інформаційну систему та її ресурси. Даний термін може визначати, як дії зловмисника націлені на отримання контролю над ІКСМ, негативного впливу на критичні властивості інформації в мережі компанії. Крім того можна сказати, що атака являє собою реалізацію вразливості мережі. Тобто, якщо говорити більш глобально то, атака це послідовність дій спрямована на реалізацію вразливості, або вразливостей ІКСМ, з метою її контролю.

Існують різні методи класифікації атак [2]. Наприклад, виділення пасивних і активних, зовнішніх і внутрішніх, промислових і непромислових. Однак, нижче надана більш узагальнена класифікація видів атак, з коротким описом їх реалізації.

1) Віддалене проникнення – вибір інформаційних атак, які дозволяють реалізувати віддалене управління комп'ютером користувачів інформаційних ресурсних систем по мережах на базі віддаленого доступу.

2) Локальне проникнення – атака, яка відбувається з внутрішньої сторони мережі, зазвичай яка призводить до несанкціонованого доступу до узлу ІКСМ, на якому вона запущена.

3) Віддалена відмова в наданні послуги – атака, яка перевантажує систему ззовні шляхом постійної відправки даних, які система не може опрацювати. При вдалій атаці система зупиняється або повністю перезавантажується.

4) Місцева відмова в обслуговуванні – атака, яка легко зупиняє функціонування систему на якій вона реалізується.

5) Мережні сканери – програми, які аналізують топологію мереж і обнаруживают сервіси, доступні для атаки. Приміром такої програми можна назвати систему nmap.

6) Сканери вразливостей – програми, що здійснюють пошук, уявляють себе на підключених мережах, і можуть бути використані для здійснення дій.

7) Зломщики паролів – програми, які підбирають паролі авторизованих користувачів, користуються інформаційними ресурсами, і її послуга.

8) Аналізатори протоколів – програми, які прослуховують мережний трафік. З підтримкою цих програм можна автоматично знайти таку інформацію, як ідентифікатори та паролі користувачів, інформацію про кредитні карти та ін.

Останнім часом стала популярною атака під назвою «водопій». Заключається вона в тому щоб замість того, щоб ламати компанії-жертви, на які вони орієнтують свої зусилля, а таких компаній може бути багато (одиниці, десятки або навіть сотні), іноді досить зламати всього лише одного виробника програмного забезпечення, з сайту якого потім всі починають завантажувати оновлення програмного забезпечення (нові прошивки, патчі, апдейти або нові версії софта). Якщо зламали саме виробника, то далі разом з цими оновленнями, які викачуються з його сайту, можливо розмістити в мережі компанії-жертви ще й шкідливий код, який потім полегшує хакерам розвиток можливості атак всередині вже скомпрометованої мережі жертвою.

Також слід звернути увагу, що одне з найслабших місць в будь-якому захисті – самі співробітники, які можуть проігнорувати попередження антивірусного ПО і додати в білий список шкідливе програмне забезпечення.

Спам розсилки часто застосовуються для проведення фішинг атак, що використовуються для впровадження вірусу або іншого шкідливого ПЗ в корпоративну мережу. Користувачі, які щодня обробляють велику кількість електронної пошти, більш часто стають жертвами фішинг-повідомлень. Тому завдання ІТ-відділу компанії – відфільтрувати максимальну кількість спаму із загального потоку електронної пошти [3]. Ця задача вирішується шляхом фільтрації спаму. До основних способів фільтрації спаму можна віднести:

- спеціалізовані постачальники сервісів фільтрації спаму;
- ПЗ для фільтрації спаму на власних поштових серверах;
- спеціалізовані апаратні рішення, розгорнуті в корпоративному дата-центрі.

Далі будуть наведені основні види атак на комп’ютерні мережі та механізми боротьби з ними.

Підміна address resolution protocol (ARP) – це атака, відома також під ім'ям ARP Redirect, перенаправляє мережевий трафік від однієї або більше машин до машини зловмисника. Виконується у фізичній мережі жертви [3].

Протокол реалізує механізм дозволу IP-адрес в MAC-адреси Ethernet. Мережне обладнання спілкується між собою шляхом обміну Ethernet-фреймів, на канальному рівні. Для забезпечення можливості передачі цієї інформації необхідно, щоб кожен мережевий інтерфейс мав свій унікальний адресу в мережі Ethernet, він і називається MAC-адресою.

При посилці IP-пакета, що відправляє машина повинна знати MAC-адресу одержувача. Щоб його дізнатися, в локальну мережу надсилається широкомовний ARP-запит. Машина з відповідним IP-адресою відповідає ARP-пакетом, що містить запитаний MAC-адресу. З цього моменту, що відправляє машина знає MAC-адресу відповідний IP-адресою призначення. Це відповідність зберігається деякий час в кеші.

Вже згадана атака змінює кеш цільової машини. Зловмисник надсилає ARP-відповіді цільової машині з інформацією про новий MAC-адресу, відповідному IP-адресою шлюзу. Насправді, цей MAC-адресу відповідає інтерфейсу машини зловмисника. Отже, весь трафік до шлюзу буде тепер отримувати машина зловмисника. Тепер можна прослуховувати трафік і змінювати його. Після цього, трафік буде направлятися до реального цільовим адресою і таким чином ніхто не помітить змін.

Атака ARP Spoofing використовується в локальній мережі, побудованої на комутаторах. З її допомогою можна перенаправити потік ethernet-фреймів на інші порти, відповідно до MAC-адрес. Після чого зловмисник може перехоплювати всі пакети на своєму порту. Таким чином, атака ARP Spoofing дозволяє перехоплювати трафік машин, розташованих на різних портах комутатора.

Переповнення буфера одна з найстарших атак в області комп'ютерної безпеки. За своєю суттю, переповнення буфера є неймовірно простою вразливістю, що реалізується дуже часто. Комп'ютерні програми часто працюють з блоками даних, що читаються з диска, з мережі, або навіть з клавіатури. Для розміщення цих даних, програми виділяють блоки пам'яті

кінцевого розміру – буфери. Переповнення буфера відбувається, коли відбувається запис або читання обсягу даних більшого, ніж вміщує буфер [3].

Переповнення буфера створює проблеми тільки в нативному коді, тобто в таких програмах, які використовують набір інструкцій процесора безпосередньо, без посередників на зразок Java або Python. Переповнення пов'язані з тим як процесор і програми в нативному коді управляють пам'яттю. Різні операційні системи мають свої особливості, але всі сучасні поширені платформи слідують загальним правилам. Щоб зрозуміти, як працюють атаки, і які бувають способи протидії, спочатку треба розглянути як в комп’ютрних пристроях реалізовано використання пам'яті.

Найважливішою концепцією є адреса в пам'яті. Кожен окремий байт пам'яті має відповідний числовий адресу. Коли процесор читає або записує дані в основну пам'ять, тобто random access memory (RAM) або read-only memory (ROM), він використовує адресу пам'яті того місця, звідки відбувається зчитування або куди проводиться запис. Системна пам'ять використовується не тільки для даних, також використовується для розміщення виконуваного коду, з якого складається програма. Це означає, що кожна з функцій запущеної програми також має адресу.

Спочатку, процесори і операційні системи використовували адреси фізичної пам'яті: кожен адреса пам'яті безпосередньо співвідносився з адресою конкретного шматка RAM. Хоча, деякі частини сучасних операційних систем все ще використовують фізичні адреси, всі сучасні операційні системи використовують схему, яка називається віртуальної пам'ятю.

При використанні віртуальної пам'яті, пряме відповідність між адресою пам'яті і фізичним ділянкою RAM відсутня. Замість цього, програми і процесор оперують у віртуальному просторі адрес. Операційна система і процесор спільно підтримують відповідність між адресами віртуальної і фізичної пам'яті.

Оскільки кожен процес отримує свій власний набір адрес, ця схема є простим способом запобігти пошкодженню пам'яті одного процесу іншим: всі адреси до яких процес може звертатися належать тільки йому. Це набагато простіше і для самого процесу, оскілки адреси фізичної пам'яті, мають особливості, які роблять їх кілька незручними у використанні.

Говорячи загалом, існують чотири поширених об'єкта, три з яких представляють для зловмисника інтерес. Нецікавий для нього блок, в більшості

операційних систем – ядро операційної системи. В інтересах продуктивності, адресний простір зазвичай поділяють на дві половини, нижня з яких використовується програмою, а верхня займається адресним простором ядра. Половина, віддана ядру, недоступна з половини зайнятої програмою, однак саме ядро може читати пам'ять програми. Це є одним із способів передачі даних у функції ядра.

В першу чергу потрібно розібратися з виконуваної частиною і бібліотеками. Головний виконуваний файл і всі його бібліотеки завантажуються в адресний простір процесу, і всі складові їх функції, таким чином, мають адресу в пам'яті.

Друга частина використовуваної програмою пам'яті використовується для зберігання оброблюваних даних і зазвичай називається купою. Ця область, наприклад, використовується для зберігання редагованого документа, або веб-сторінки, (з усіма її об'єктами JavaScrit, CSS і т.п.).

Третя і найважливіша частина – стек викликів, зазвичай званий просто стеком. Це найскладніший аспект. Кожен потік в процесі має свій стек. Це область пам'яті, яка використовується для одночасного відстеження як поточної функції виконується в потоці, так і всіх попередніх функцій тих, що були викликані, щоб потрапити в поточну функцію.

Стек викликів є спеціалізованою версією структури даних, званої «стеком». Стеки є структурами змінної довжини, призначеними для зберігання об'єктів. Нові об'єкти можуть бути додані в кінець стека (зазвичай званого «вершиною» стека) і об'єкти можуть бути зняті зі стека. Тільки вершина стека підлягає зміні з використанням push і pop, таким чином, стек встановлює суворий порядок сортування: об'єкт, який останнім поклали в стек, буде тим, який буде знятий з нього наступним.

Найважливішим об'єктом, що зберігається в стеку викликів, є адреса повернення. У більшості випадків, коли програма викликає функцію, ця функція виконує те, що повинна (включаючи виклик інших функцій), а потім повертає керування в функцію, яка її викликала. Для повернення, до викликання функції необхідно зберегти запис про неї: виконання має продовжитися з інструкції наступною після інструкції виклику. Адреса цієї інструкції називається адресою повернення. Стек використовується для зберігання цих адрес повернення, тобто при кожному виклику функції, в стек поміщається адреса повернення. При

кожному повернення, адреса знімається зі стека і процесор починає виконувати інструкцію по цій адресі.

Стекова функціональність є настільки базовою і необхідною, що більшість, якщо не всі процесори мають вбудовану підтримку цих концепцій. Візьмемо за приклад процесори x86. Серед регістрів, визначених у специфікації x86, два найбільш важливих – extended instruction pointer (EIP) і extended stack pointer (ESP).

ESP завжди містить адресу вершини стека. Кожен раз коли щось додається в стек, значення ESP зменшується. Кожен раз, коли щось знімається зі стека, значення ESP збільшується. Це означає, що стек росте вниз, це означає, що у міру додавання об'єктів в стек, адреса зберігається в esp стає все менше і менше. Незважаючи на це, область пам'яті, на яку вказує ESP, називається вершиною стека.

Якби стек викликів зберігав тільки набір адрес повернення, проблеми б не було. Реальна проблема приходить з усім іншим, що кладуть в стек. Так виходить, що стек – це швидке і ефективне місце зберігання даних. Зберігати дані в купі складно, бо програма повинна відстежувати доступне в купі місце, скільки займає кожен з об'єктів та інше. При цьому робота зі стеком проста, щоб розмістити трохи даних, досить просто зменшити значення покажчика. А щоб почистити за собою, досить збільшити значення покажчика.

Це зручність робить стек логічним місцем для розміщення змінних, використовуваних функцією. Функції потрібно 256 байт буфера, щоб прийняти введення користувача для цього просто віднімається 256 від покажчика стека і буфер готовий. В кінці функції, просто додається 256 до покажчика, і буфер буде відкинутий.

Однак, у такого підходу існують обмеження. Стек не підходить для зберігання дуже великих об'єктів: загальний обсяг доступної пам'яті звичайно фіксований при створенні потоку і, часто, становить приблизно 1 МБ в обсязі. Тому великі об'єкти повинні бути поміщені в купу. Стек також застосовується для об'єктів, які повинні існувати довше, ніж виконується одна викликана функція. Оскільки всі розміщення в стеку видаляються при виході з функції, час життя будь-якого з об'єктів в стеку не перевищує часу виконання відповідної функції. На об'єкти в купі це обмеження не поширюється, вони можуть існувати "вічно".

Якщо переходити до класифікації атак переповнення буферу, то виходячи з підзадач, реалізацію яких вимагає атака, виділяють наступні способи боротьби з атаками подібного типу.

Наприклад, можливо коригувати вихідні коди програми для усунення вразливостей. Переповнення буфера відбувається, перш за все, через неправильне виконання алгоритму роботи програми, який не передбачає перевірок виходу за межі буферів. Також можливе застосування спеціальних утиліт автоматичного пошуку вразливостей в вихідному коді програми. Зазначені методи і засоби дозволяють створювати більш захищені програми, але не вирішують проблему в принципі, а лише мінімізують число вразливостей по переповнення буфера. Даний підхід орієнтований безпосередньо на розробників програмного забезпечення і не є інструментом кінцевого користувача або системного адміністратора.

Крім того, є можливим використання нездійсненних буферів. Суть методу полягає в забороні виконання коду в сегментах даних і стека, тобто параметри сегментів даних і стека містять тільки атрибути запису і читання, але не виконання. Однак обмеження на виконання даних призводить до проблеми несумісності. Виконуваний стек необхідний для роботи багатьох програм, так як на його основі генерується код компіляторами, реалізуються системні функції операційних систем, реалізується автоматична генерація коду. Захист з використанням нездійсненних буферів запобіжить тільки атаки з впровадженням коду, але не допоможе при інших видах атак.

Також можна застосування перевірки виходу за межі буферу. В основі цього методу лежить виконання перевірок виходу за межі змінної при кожному зверненні до неї. Це запобігає всі можливі атаки по переповнення буфера, так як повністю виключає саме переповнення. Однак, у цього рішення є істотний недолік – значне зниження продуктивності програми.

У тому числі можливе застосування перевірок цілісності. При цьому вводиться поняття так званого квазі-сталості, тобто стану середовища, яке незмінно в певних рамках. Така квазі-сталість дозволяє усунути ряд надлишкового коду перевірки виконання різних умов.

Використання спеціалізованих програм. Робочі станції кінцевих користувачів дуже уразливі для вірусів і троянських коней. Вірусами називаються шкідливі програми, які впроваджуються в інші програми для виконання певної

небажаної функції на робочій станції кінцевого користувача. Як приклад можна привести вірус, який прописується у файлі command.com (головному інтерпретаторі систем Windows) і стирає інші файли, а також заражає всі інші знайдені ним версії command.com.

Сніффер пакетів є прикладною програмою, яка використовує мережеву карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому сніффер перехоплює всі мережні пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніфферів можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення імен і паролів створює велику небезпеку, так як користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і додатків. Якщо додаток працює в режимі клієнт-сервер, а аутентифікаційні дані передаються по мережі в текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів [3].

Rootkit – програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі [3]. Більшість з реалізацій сучасних rootkit можуть ховати від користувача файли, папки і ключі реєстру, приховувати запущені програми, системні служби, драйвери і мережеві з'єднання. Тобто зловмисник має можливість створювати файли і ключі реєстру, запускати програми, працювати з мережею і ця активність не буде виявлена адміністратором. Крім того, rootkits можуть приховувати мережеву активність шляхом модифікації стека протоколів TCP / IP. Тобто якщо в системі встановлено Web-сервер, і відповідно відкритий 80 порт, rootkit може використовувати його для взаємодії з хакером, в той час як інші користувачі будуть без проблем працювати по протоколу HTTP.

Для боротьби з цією атакою можна використовувати антивірусні засоби а також регулярно оновлювати їх сигнатури. Дане рішеня може вирішити проблему

з троянськими програмами, вірусами, поштовими хробаками, але не вирішить проблему сніфферов і rootkit-ів. Також можна використовувати шифрування даних, що передаються. Проблема не вирішує повністю проблему сніфферів, однак, противник перехоплює дані, які не можна вільно прочитати. Для їх розшифровки потрібен час.

Мережною розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі зловмисник, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів domain name system (DNS), exo-тестуванням і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласненні [3].

Exo-тестування адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі [3]. Отримавши список хостів, зловмисник використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами. І, нарешті, зловмисник аналізує характеристики додатків, що працюють на хостах. В результаті видобувається інформація, яку можна використовувати для злому. Для того щоб перешкоджати даній атаці потрібно відключити відлуння ICMP і exo-відповідь на периферійних маршрутизаторах. Однак це, призведе до втрати даних необхідних для діагностики мережевих збоїв, також можна використовувати системи виявлення вторгнень (IDS).

IP-спуфінг відбувається, коли зловмисник, що знаходиться всередині компанії або поза нею видає себе за санкціонованого користувача [3]. Це можна зробити двома способами. По-перше, зловмисник може скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або вповноваженим зовнішнім адресою, якому дозволяється доступ до певних мережевих ресурсів. Атаки IP-спуфінга часто є відправною точкою для інших атак.

Класичний приклад – атака denail of service (DoS), яка починається з чужої адреси, що приховує справжню особу зловмисника. Зазвичай IP-спуфінга обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним додатком або по каналу зв'язку між однорангових пристроями. Для двостороннього зв'язку зловмисник повинен змінити все таблиці маршрутизації, щоб направити трафік на свої IP-

адреси. Деякі зловмисники, однак, навіть не намагаються отримати відповідь від додатків.

Якщо головне завдання полягає в отриманні від системи важливого файлу, відповіді додатків не мають значення. Якщо ж зловмиснику вдається змінити таблиці маршрутизації і направити трафік на свої IP-адреси, зловмисник отримає всі пакети і зможе відповідати на них так, ніби він є санкціонованим користувачем. Загрозу IP-спуфінга можна послабити (але не усунути) за допомогою контролю доступу.

Найпростіший спосіб запобігання IP-спуфінга полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфінга, потрібно налаштувати контроль доступу на відсікання будь-якого трафіку, що надходить із зовнішнього мережі з вихідною адресою, яка повинна розташовуватися всередині локальної мережі. Якщо санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає неефективним. Також можна використовавати фільтрацію RFC 2827. Для цього необхідно бракувати будь-який вихідний трафік, початкова адреса якого не є одним з IP-адрес компанії. Цей тип фільтрації може виконувати і провайдер. В результаті відбраковують весь трафік, який не має вихідного адреси, очікуваного на певному інтерфейсі, також можна використовувати криптографічну аутентифікацію.

Для атаки типу Man-in-the-Middle зловмисникові потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто використовуються сніфери пакетів, транспортні протоколи і протоколи маршрутизації. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії. Для боротьби з цим типом атаки достатньо використовувати шифрування даних.

Structured query language (SQL)-ін'єкція – це атака, в ході якої змінюються параметри SQL-запитів до бази даних [3]. В результаті запит набуває зовсім інший зміст, і в разі недостатньої фільтрації вхідних даних здатний не тільки зробити висновок конфіденційної інформації, а й змінити або видалити дані. Для

захисту від даної загрози адміністратори ресурсів можуть вставити систему стеження за SQL-ін’єкціями.

PHP-ін'єкція – один із способів злому веб-сайтів, що працюють на PHP. Він полягає в тому, щоб впровадити спеціально сформований зловмисний сценарій в код веб-додатків на серверній стороні сайту, що призводить до виконання довільних команд.

Міжсайтовий скриптинг – це атака на вразливість, яка існує на сервері, що дозволяє впровадити в створювану сервером HTML-сторінку якийсь довільний код, в якому може бути взагалі все що завгодно і передавати цей код в якості значення змінної [3]. Значення цієї змінної передається від створюваної HTML-сторінки на сервер в скрипт і далі іде виклик шляхом відправки запиту. PHP-скрипт у відповідь на даний запит генерує HTML-сторінку, в якій відображаються значення потрібних зловмисникові змінних, і відправляє цю сторінку на браузер зловмисника.

Тобто, кажучи простіше, XSS атака – це атака за допомогою вразливостей на сервері на комп'ютери клієнтів. XSS атака найчастіше використовується для крадіжки Cookies. У них зберігається інформація про сесії перебування користувача на сайтах, що і буває потрібним зловмисникам для перехоплення управління особистими даними користувача на сайті в межах, поки сесія не буде закрита сервером, на якому розміщений сайт. Крім цього в Cookies зберігається зашифрований пароль, під яким користувач входить на даний сайт, і при наявності необхідних утиліт і бажання зловмисникам не дуже важко розшифрувати даний пароль.

XSS атака може бути проведена не тільки через сайт, але і через уразливості в програмному забезпеченні, зокрема через браузери. Тому рекомендується оновлювати використовується програмне забезпечення. Також можливе проведення XSS атак через використання SQL-коду. Як ми бачимо з усього вищесказаного, можливостей у XSS атак досить багато. Зловмисник може опанувати вашою особистою інформацією аж до отримання паролів доступу до сайтів, а це дуже неприємно. До того ж XSS атака завдає шкоди виключно клієнтським машинам, залишаючи сервер в повністю робочому стані, і у адміністрації різних серверів часом мало стимулів встановлювати захист від цього виду атак.

Розрізняють XSS атаки двух видів: активні і пасивні. При першому виді атаки шкідливий скрипт зберігається на сервері і починає свою діяльність при завантаженні сторінки сайту в браузері клієнта. При другому виді атак скрипт не зберігається на сервері і шкідливий вплив починає виконуватися тільки в разі будь-якого дії користувача, наприклад, при натисканні на сформовану посилання.

XPath-ін'єкція – вид вразливостей, який полягає у впровадженні XPath-виразів в оригінальний запит до бази даних XML [3].

Для боротьби з XPath-ін'єкцією насамперед адміністратори ресурсів повинні незалежно від програми, середовища або мови програмування необхідно дотримуватися наступних практичних правил:

- припускати, що всі дані сумнівні;
- перевіряти дані на стороні клієнта;
- перевіряти дані на стороні Web-сервера;
- дотримуватись послідновної стратегії захищеності додатків;
- тестувати додаток на відомі загрози перед його запуском.

Відмова в обслуговуванні (DoS), поза всяким сумнівом, є найбільш відомою формою атак [3]. Крім того, проти атак такого типу найважче створити стовідсотковий захист. Проте, саме простота реалізації і величезний яку завдають шкоди залучають до DoS пильну увагу адміністраторів, що відповідають за мережеву безпеку. Атаки DoS відрізняються від атак інших типів. Вони не націлені на отримання доступу до вашої мережі або на отримання з цієї мережі будь-якої інформації. Атака DoS робить вашу мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

У разі використання деяких серверних додатків атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів.

В ході атак DoS можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP (Internet Control Message Protocol). Більшість атак DoS спирається не на програмні помилки або проломи в системі безпеки, а на загальні слабкості системної архітектури. Деякі атаки зводять до нуля продуктивність мережі, переповняючи її небажаними і непотрібними пакетами або повідомляючи помилкову інформацію про поточний стан мережевих ресурсів.

Цей тип атак важко запобігти, так як для цього потрібно координація дій з провайдером. Якщо трафік, призначений для переповнення вашої мережі, не зупинити у провайдера, то на вході в мережу ви це зробити вже не зможете, тому що вся смуга пропускання буде зайнята. Коли атака цього типу проводиться одночасно через безліч пристроїв, ми говоримо про розподіленої атаки DoS (DDoS - distributed DoS).

Для того щоб знизити загрозу Dos-атак можна скористатися функціями анти-спуфінга. Правильна конфігурація функцій анти-спуфінга на маршрутизаторах і міжмережевих екранах допоможе знизити ризик DoS. Ці функції, як мінімум, повинні включати фільтрацію RFC 2827. Також можна використовувати функцію анти-DoS. Правильна конфігурація функцій анти-DoS на маршрутизаторах і міжмережевих екранах може обмежити ефективність атак. Ці функції часто обмежують число напіввідкритих каналів в будь-який момент часу. Також принести успіх функція обмеження обсягу трафіку. Організація може попросити провайдера обмежити обсяг трафіку. Цей тип фільтрації дозволяє обмежити обсяг некритичного трафіку, що проходить по вашій мережі.

Фішинг-атаки – процес обману або соціальна обробка клієнтів організацій для подальшої крадіжки їх ідентифікаційних даних та передачі їх конфіденційної інформації для злочинного використання [3]. Злочинці для свого нападу використовують спам або комп'ютери-боти. При цьому розмір компанії-жертви не має значення, якість особистої інформації отриманої злочинцями в результаті нападу, має значення саме по собі.

Кращий захист від фішинг-атак – це використовувати тільки перевірені ресурси і шляхи доступу до них, також використовувати антивірусні засоби та обов’язково оновлювати їх сигнатури.

Однією з різновидів несанкціонованих програм є комп'ютерні віруси, кількість яких постійно зростає, уже є навіть нова інженерна дисципліна - комп'ютерна вірусологія.

Наслідки впливу вірусів можуть бути різноманітними; від зовні незвичайних ефектів на моніторі і простого уповільнення роботи до краху обчислювальних системи або мережі. Звідси виникає необхідність захисту від вірусів на всіх стадіях їх розвитку, проникнення в систему і розмноження.

Для цього в систему захисту включають програмно-апаратні засоби, використовують різні антивірусні програми для локалізації і видалення вірусів і

усунення наслідків їх впливу. На сьогоднішній день склалися усталені назви для деяких типів вірусів. Наприклад пастками називаються віруси, що використовують наявні неточності в діючих програмах або недосконаліть (наприклад, змінюють адресу входу з програми в програми і назад).

Логічні бомби або бомби уповільненої дії здійснюють тривалу і різноманітну підготовку до проведення деструктивних дій і потім спрацьовують при виконанні певного етапу робіт, в спрацьовує, зверненого до програми певного користувача. Ці віруси особливо небезпечні в силу тривалості періоду часу, при якому вони себе практично не виявляють, хоча вже ведуть руйнівну роботу.

Віруси-черв'яки викликають некероване функціонування, наприклад, мережевих або периферійних пристроїв (нескінченний «прогін» паперу в принтері; постійну перезавантаження ОС і т.п.).

Троянськими кіньми називаються віруси, поширювані разом з ПО спеціального призначення, причому для користувача виявляються вкрай несподіваними їх дії (наприклад, таким вірусів можуть бути зараженими самі антивірусні програми).

Боротьба з вірусами ведеться шляхом застосування програм-антивірусів, які здійснюють виявлення або виявлення і видалення вірусу. Мережеві віруси займають особливе місце серед безлічі відомих вірусів.

Можливість шифрування вірусами корпоративних мереж стає серйозною проблемою. Небезпека дії вірусів визначається можливістю часткової або повної втрати цінної інформації, а також втратою часу і коштів, спрямованих на відновлення нормального функціонування ІС [3].

Основні шляхи, якими файли, заражені вірусами, потрапляють в корпоративну мережу наведені нижче.

1) Копіювання інфікованих файлів або при запуску програм і інших файлів перенесених на носіях інформації(гнучких, оптичних дисків і т.д.).

2) Програмне забезпечення, отримане через WEB або FTP і збережене на локальних робочих станціях.

3) Файли, одержувані при з'єднанні віддаленого сервера з мережею для обміну з файловим сервером.

4) Електронна пошта, яка містить прикладені заражені файли.

Мережеві віруси для свого поширення активно використовують протоколи і можливості локальних і глобальних мереж.

Основним принципом роботи мережного вірусу є можливість самостійно передати свій код на віддалений сервер або робочу станцію і можливістю запустити на виконання свій код на віддаленому комп'ютері або «підштовхнути» користувача до запуску зараженого файлу.

Важливо зрозуміти, що мережна безпека – це еволюційний процес. Немає жодного продукту, здатного надати корпорації повну безпеку. Надійний захист мережі досягається поєднанням продуктів і послуг, а також грамотною політикою безпеки і її дотриманням усіма співробітниками від верху до низу. Можна помітити, що правильна політика безпеки навіть без виділених коштів захисту дає кращі результати, ніж засоби захисту без політики безпеки.

Таким чином, були розглянуті основні мережеві атаки і способи боротьби з ними. Дана область є найбільш розвивається, так як йде постійне суперництво між зловмисниками і організаціями, що забезпечують безпеку даних. Незважаючи на можливе вжиття комплексних заходів щодо захисту комп'ютера, найбільш надійним способом захисту комп'ютера є використання перевірених електронних ресурсів, читання листів з перевірених джерел. Тобто найбільший захист від атак може забезпечити сам користувач, дотримуючись запобіжних заходів.

2 ВИЗНАЧЕННЯ ІМОВІРНОСТІ ПОРУШЕННЯ КРИТИЧНИХ ВЛАСТИВОСТЕЙ ІНФОРМАЦІЙНОГО АКТИВУ НА ОСНОВІ CVSS. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1 Класифікація інформації на підприємстві

Інформацію можна класифікувати за кількома видами і залежно від категорії доступу до неї поділяється на загальнодоступну інформацію, а також на інформацію, доступ до якої обмежено, тобто конфіденційні дані і державна таємниця [4].

Інформація в залежності від порядку її надання або поширення поділяється на інформацію вільно поширювану та інформацію з обмеженим доступом, яка поділяється на:

- конфіденційна інформація;
- таємна інформація;
- службова інформація.

Інформація за призначенням буває наступних видів.

1) Масова – містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму.

2) Спеціальна – містить специфічний набір понять, які можуть бути не зрозумілі основній масі соціуму, але необхідні і зрозумілі в рамках вузької соціальної групи, де використовується дана інформація.

3) Секретна – доступ, до якої надається вузькому колу осіб і за закритими (захищеним) каналам.

4) Особиста – набір відомостей про яку-небудь особистості, що визначає соціальний стан і типи соціальних взаємодій.

Конфіденційною є інформація про фізичну або юридичну особу, крім суб’єктів владних повноважень, яка обмежена у доступі цією особою, а також попередньо обмежена законодавством до моменту, поки особа не відкриє таку інформацію за власним бажанням.

Така інформація може поширюватися за згодою відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших

випадках, визначених закономзаконодавством може бути заборонено віднесення певної інформації до обмеженої у доступі, зокрема і конфіденційної.

Засоби захисту інформації необхідно застосовувати безпосередньо до інформації доступ до якої обмежено – це державна таємниця і конфіденційні дані.

Перше, що важливо запам'ятати персональні дані – це завжди інформація про фізичну особу, відповідно до статей 24 і 25 Цивільного кодексу України людина як учасник цивільних відносин вважається фізичною особою. Її цивільна правоздатність виникає в момент народження і припиняється в момент смерті. Тому, враховуючи положення Закону «Про захист персональних даних» і Цивільного кодексу, інформація про померлу особу не є її персональними даними.

Однак, до конфіденційної може відноситись також інформація про юридичну особу, наприклад, "комерційна таємниця". Відповідно до статті 505 Цивільного кодексу України це можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру (за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці) і щодо яких ця юридична особа вжила заходи щодо збереження секретності. До конфіденційної юридичною особою може бути віднесена також і інша інформація.

В той же час законодавством може бути заборонено віднесення певних персональних даних фізичної особи до конфіденційної інформації. Відкритою є наступна інформація.

1) Прізвища, імена, по батькові фізичних осіб, які отримали бюджетні кошти, отримали у володіння, користування чи розпорядження державне та/або комунальне майно (частина п'ята статті 6 Закону «Про доступ до публічної інформації»).

2) Персональні дані, що стосуються здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень (частина друга статті 5 Закону «Про захист персональних даних». На рис. 2.1 зображена класифікація інформації в Україні.

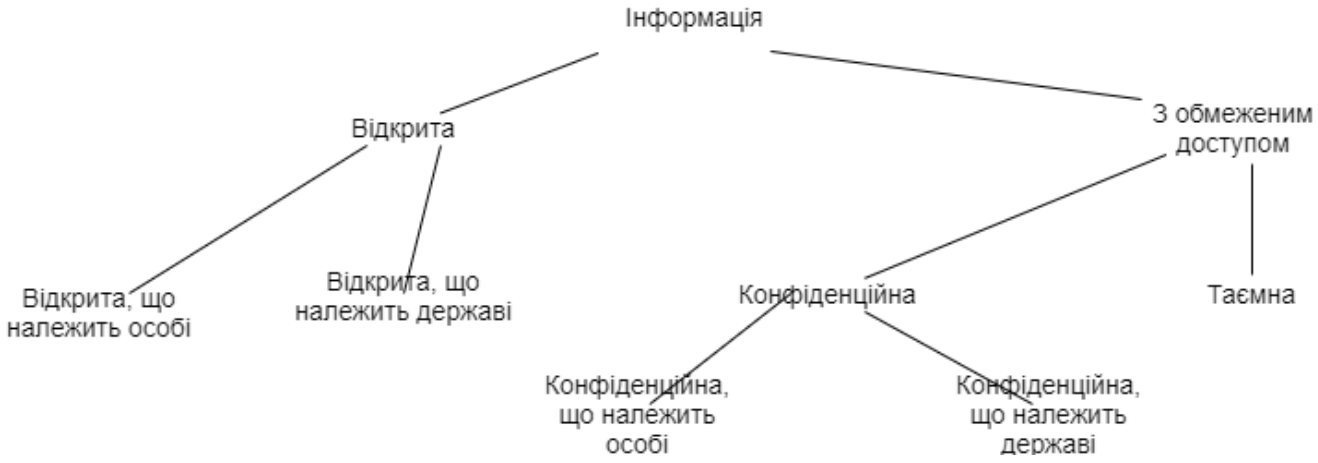

Рисунок 2.1 – Класифікація інформації в Україні

Для того щоб забезпечити безпеку і конфіденційність інформації необхідно визначити які бувають носії інформації, доступ до яких буває відкритим і закритим. Відповідно способи і засоби захисту підбираються так само в залежності і від типу носія [4]. Основні носії інформації описані нижче.

1) Друковані та електронні засоби масової інформації, соціальні мережі, інші ресурси в інтернеті.

2) Співробітники організації, у яких є доступ до інформації на підставі своїх дружніх, сімейних, професійних зв'язків.

3) Засоби зв'язку, які передають або зберігають інформацію: телефони, АТС, інше телекомунікаційне обладнання.

4) Документи всіх типів: особисті, службові, державні.

5) Програмне забезпечення як самостійний інформаційний об'єкт, особливо якщо його версія допрацьовувалася спеціально для конкретної компанії.

6) Електронні носії інформації, які обробляють дані в автоматичному порядку.

Визначивши, яка інформація підлягає захисту, носії інформації і можливі збитки при її розкритті, Ви можете підібрати необхідні засоби захисту.

2.2 CVSS метрики

Останнім часом все більше конфіденційної інформації зберігається і обробляється в різних інформаційних системах (ІС). Практично будь-який ІС

притаманні уразливості, які обумовлюють можливість реалізації загроз оброблюваної в ній інформації.

Процес управління вразливостями включає виявлення, класифікацію, оцінку і усунення вразливостей. Для виявлення вразливостей використовуються спеціальні програмні і апаратні засоби, звані сканерами вразливостей.

Більшість сучасних сканерів вирішують також завдання класифікації знайдених вразливостей, використовуючи дані з певної бази вразливостей, наприклад Common Vulnerabilities and Exposures (CVE). Існують різні системи оцінки вразливостей. Найбільш поширена і перевірена на практиці CVSS. У CVSS для кожної уразливості розраховується базова оцінка в інтервалі від 0 до 10. Потім визначається рівень небезпеки уразливості за спеціальною шкалою. Таким чином, CVSS дозволяє ранжувати знайдені вразливості і визначати пріоритети їх усунення.

Деякі уразливості усуваються за допомогою патчів. Використання патчів можливо в тому випадку, якщо виробником програмного забезпечення (ПЗ) було випущено оновлення, що дозволяє усунути виявлену уразливість. Якщо таке оновлення не було випущено, то вразливість можна частково або повністю усунути за рахунок використання додаткових заходів і засобів захисту, що, в свою чергу, вимагає певних фінансових витрат. Тому особливо гостро стоїть задача визначення ефективності їх застосування для усунення виявлених вразливостей. Для вирішення даного завдання пропонується використовувати ризик-орієнтований підхід.

Данний підрозділ буде присвячений розробці методу для визначення ймовірності порушення критичних властивостей інформаційного активу на основі CVSS метрик вразливостей. Даний метод дозволить оцінити ризик, пов'язаний з експлуатацією вразливостей ІС, і визначити ефективність використання додаткових заходів і засобів захисту для їх усунення.

Згідно найбільш поширеній підходу, зафіксованому в стандарті ISO / IEC 27005, значення ризику (R) може бути визначено за формулою:

$$R = \sum_{j=1}^{n} P_r^j \cdot I^j, \qquad (2.1)$$

де P_r^j – ймовірність реалізації j-й загрози;

I^j – значення збитку від реалізації j-й загрози;

n – число загроз.

Формула (2.1) універсальна для всіх типів об'єктів захисту, до яких можуть належати інформаційні активи (ІА), ПЗ, технічні засоби (ТЗ) та інші.

У стандарті NIST 800-37 представлений трирівневий підхід до оцінки ризику, відповідно до якого виділяють рівень ІС, рівень бізнес-процесів і рівень організації. На рівні ІС відбувається ідентифікація ІА, вразливостей і загроз, а також застосовуваних засобів і заходів захисту. Цієї інформації достатньо для визначення ймовірності виникнення збитків.

Величина збитку визначається переважно на рівнях бізнес-процесів і організації з залученням власників бізнес-процесів, керівництва компанії та інших зацікавлених осіб. На даному етапі дослідження завдання визначення величини збитку від порушення властивостей ІА не ставиться, що дозволяє не розглядати два верхніх рівня підходу, представленого в NIST 800-37, а зупинитися на рівні ІС.

Процес забезпечення інформаційної безпеки спрямований на забезпечення критичних властивостей ІА, до яких найчастіше відносять конфіденційність, цілісність і доступність. У методі пропонується окремо визначати значення ризику від втрати конфіденційності, цілісності та доступності ІА. При цьому сума значень ризику, пов'язаних з втратою окремих критичних властивостей ІА, становитиме повний ризик ІА. З урахуванням цього формула для визначення величини повного ризику ІА (R) набуває вигляду:

$$R = P_c \cdot I_c + P_i \cdot I_i + P_a \cdot I_a, \qquad (2.2)$$

де P_c – ймовірність порушення конфіденційності ІА;

I_c – значення збитку, що виникає при порушенні конфіденційності ІА;

P_i – ймовірність порушення цілісності ІА;

I_i – значення збитку, що виникає при порушенні цілістності ІА;

P_a – ймовірності порушення доступності ІА;

I_a – значення збитку, що виникає при порушенні доступності ІА.

Перевага даного підходу в тому, що немає необхідності для кожної пари «загроза-вразливість» визначати значення збитку. Це дозволяє окремо оцінювати ймовірності порушення критичних властивостей ІА і значення збитку від порушення цих властивостей.

Зазвичай при оцінці ризику спочатку визначається перелік актуальних загроз, а уразливості лише характеризують можливість їх реалізації. У пропонованому методі акцент зміщується з загроз на уразливості. Замість ймовірності реалізації загрози визначається ймовірність експлуатації уразливості, яка враховує як ймовірність наявності уразливості, так і ймовірність її використання хоча б однією із загроз.

Сам факт успішної експлуатації уразливості не обов'язково тягне за собою порушення критичних властивостей ІА. Тому для кожної уразливості необхідно визначати ймовірності того, що її експлуатація призведе до порушення критичних властивостей ІА. Вважається, що уразливості незалежні один від одного, тому експлуатація однієї з них не обов'язково призведе до експлуатації інших. З огляду на це для розрахунку ймовірності порушення конфіденційності (P_c) ІА пропонуються наступні формула:

$$P_c = (1 - \prod_{j=1}^{m} (1 - P_e^j \cdot P_c^j)), \quad (2.3)$$

де P_e^j – ймовірність експлуатації j-й вразливості;

P_c^j – ймовірність порушення конфіденційності j-й вразливістю.

Формула для розрахунку ймовірності порушення цілістності (P_i) ІА:

$$P_i = (1 - \prod_{j=1}^{m} (1 - P_e^j \cdot P_i^j)), \quad (2.4)$$

де P_e^j – ймовірність експлуатації j-й вразливості;

P_i^j – ймовірність порушення цілісності j-й вразливістю.

Формула для розрахунку ймовірності порушення доступності (P_a) ІА:

$$P_a = (1 - \prod_{j=1}^{m} (1 - P_e^j \cdot P_a^j)), \quad (2.5)$$

де P_e^j – ймовірність експлуатації j-й вразливості;

P_a^j – ймовірність порушення доступності j-й вразливістю.

Використання метрик CVSS для визначення ймовірності порушення критичних властивостей ІА. Система CVSS включає три групи метрик: базові, тимчасові і контекстні. В таблиці 2.1 показано групи метрик системи CVSS з їх значеннями.

Таблиця 2.1 – Групи метрик CVSS

Базові	Тимчасові	Контексні
Вектор доступу Складність доступу Аутентифікація Вплив на конфіденціальність Вплив на цілісність Вплив доступність	Можливість використання Рівень виправлень Ступінь достовірності звіту	Імовірність непрямих збитків Щільність цілей Вимоги щодо конфіденціальності Вимоги до цілісності Вимоги до доступності

Базові метрики відображають основні характеристики уразливості, які не змінюються з часом і не залежать від середовища. Вони підрозділяються на метрики можливості експлуатації і метрики впливу. Тимчасові метрики представляють характеристики уразливості, що змінюються з часом і не залежать від середовища. Контекстні метрики представляють характеристики, пов'язані із середовищем користувача, і дозволяють оцінити рівень шкоди у відносних величинах.

У методі визначення ймовірності порушення критичних властивостей ІА використовуються базові і тимчасові метрики, значення яких визначаються аналітиками, виробниками продуктів в області ІБ або виробниками додатків. Оскільки визначення величини збитку виноситься за рамки даного дослідження, контекстні метрики в роботі не використовуються.

Таблиця 2.2 показує базові метрики можливої експлуатації, для визначення ймовірності експлуатації уразливості.

Таблиця 2.2 – Метрики, що використовуються для визначення ймовірності експлуатації уразливості

Найменування	Опис	Значення
Базові метрики CVSS		
Вектор доступа (AV)	Можливий спосіб експлуатації вразливості	Локальний (0.395) Локально-мережний(0.646) Мережний(1)
Складність доступу(AC)	Рівень складності атаки	Високий (0.35) Середній (0.61) Низький (0.71)
Аутентифікація (Au)	Спосіб аутентифікації для експлуатації вразливості	Багаторазова (0.45) Одноразова (0.56) Відстуня (0.704)
Можливість використання (E)	Наявністьабо відсутність коду чи техніки експлуатації	Неперевірений (0.85) Випробовувальний (0.9) Функціональний (0.95) Високий (1)
Рівень виправлення (RL)	Наявність або відстуність тимчасового або постійного виправлення вразливості	Офіційне виправлення (0.87) Тимчасове виправлення (0.9) Додаткові дії (0.95)
Ступінь достовірності звіту (RC)	Ступінь конфіденційності інформації стосовно існування вразливості і достовірності відомих технічних деталей	Не підтверджено (0.9) Не доведено (0.95) Підтверджено (1) Не визначено (1)

Представлені в таблиці 2.2 метрики є факторами, що впливають на ймовірність експлуатації уразливості (P_e), яка знаходиться за формулою:

$$P_e = AV \cdot AC \cdot Au \cdot E \cdot RL \cdot RC, \quad (2.6)$$

де P_e – ймовірність експлуатації уразливості;

AV – вектор доступу;

AC – складність доступу;

Au – аутентифікація;

E – можливість використання;

RL – рівень виправлення;

RC – ступінь достовірності звіту.

Для визначення ймовірності порушення критичних властивостей ІА від експлуатації уразливості використовуються базові метрики впливу і додатково вводиться метрика взаємозв'язку ІА і ПЗ, у якого була виявлена вразливість.

Так, ІА може створюватися, змінюватися, використовуватися ПО, зберігатися з ПО на одному хості, різних хостах з можливістю віддаленого доступу, або вони можуть бути не пов'язаними. Таблиця 2.3 показує базові метрики, які використовуються для визначення ймовірності порушення критичних властивостей ІА від експлуатації вразливості.

Таблиця 2.3 – Метрики, що використовуються для визначення ймовірності порушення критичних властивостей ІА від експлуатації уразливості

Найменування	Опис	Значення
1	2	3
Базові метрики CVSS		
Впливна конфіденційність(C)	Вплив вразливості на конфіденційність даних системи	Нульове (0) Часткове (0.275) Повне (0.66) Невідомо (0.66)
Вплив на цілісність (I)	Вплив вразливості на цілісність даних в системі	Нульове (0) Часткове (0.275) Повне (0.66)
Вплив на доступність (A)	Вплив вразливості на доступність системи	Нульове (0) Часткове (0.275) Повне (0,66) Невідомо (0,66)

Продовження таблиці 2.3

1	2	3
Додаткові метрики		
Залежність ІА і ПЗ (IR)	Відображає характер взаємозв'язку ІА і ПЗ, у якого була виявлена уразливість	Не зв’язані (0) Віддалене підключення (0.2) Спільне зберігання (0.4) Використання (0.6) Зміна (0.8) Створення (1) Не визначено (1)

Метрики, представлені в таблиці 2.3, є факторами, що впливають на значення ймовірностей порушення критичних властивостей ІА. З урахуванням цього ймовірності порушення конфіденційності (P_C) вираховується наступною формулою цілісності та доступності визначаються за формулами:

$$P_C = C \cdot IR, \tag{2.7}$$

де C – базова метрика впливу на конфіденційність;

IR – залежність ІА і ПЗ.

Формула для вирішеня ймовірності порушення цілісності (P_i):

$$P_i = I \cdot IR, \tag{2.8}$$

де I – базова метрика впливу на цілісність;

IR – залежність ІА і ПЗ.

Формула для вирішеня ймовірності порушення доступності (P_a):

$$P_a = A \cdot IR, \tag{2.9}$$

де A – базова метрика впливу на доступність;

IR – залежність ІА і ПЗ.

На основі чисельного значення базового вектора (V) уразливості (базової оцінки) присвоюються один з чотирьох рівнів небезпеки:

- низький рівень небезпеки, якщо $0{,}0 \leq V \leq 3{,}9$;
- середній рівень небезпеки, якщо $4{,}0 \leq V \leq 6{,}9$;
- високий рівень небезпеки, якщо $7{,}0 \leq V \leq 9{,}9$;
- критичний рівень небезпеки, якщо $V = 10{,}0$.

3 ЗАСОБИ ЗАХИСТУ МЕРЕЖ. РЕКОМЕНДАЦІЇ ЩОДО ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ

3.1 Класифікація засобів захисту мереж

Найкраща стратегія безпеки основну увагу приділяє не тільки оновленню після нещастя, скільки попередження цього нещастя. Існують наступні основні методи захисту:

- фізичні;
- організаційні;
- програмно-апаратні.

Фізичні методи захисту складаються в перешкодженні фізичного доступу сторонніх осіб в приміщення на шляху до даних і процесу їх обробки.

Організаційна захист реалізується сукупністю організаційно - технічних заходів, спрямованих на забезпечення захисту інформації, розробкою і прийняттям законодавчих актів з питань захисту інформації, затвердженням морально – етичних норм використання інформації в суспільстві. Програмно апаратні засоби захисту реалізуються наступними методами:

- програмно-апаратні шифратори мережного трафіку;
- захищені мережні криптопротоколи;
- методика Firewall;
- програмні засоби виявлення атак;
- захищені мережні операційні системи (ОС).

Використання стійкої криптографії полягає в тому, що в даний час розроблені різні протоколи обміну, що дозволяють захистити мережеве з'єднання і зашифрувати трафік.

Шифрування є досить потужним засобом захисту даних. Розшифровка вимагає знання ключа шифрування, підбір якого є трудомістким завданням.

Шифрування даних здійснюється в темпі надходження інформації і в автономному режимі.

Перший спосіб застосовується в основному в системах прийому-передачі інформації, а другий – для засекречування інформації, що зберігається.

У сучасних системах захисту в основному застосовується два алгоритму: DES і RSA.

Алгоритм DES є симетричним, тобто для шифрування і дешифрування використовується один і той же ключ. Забезпечує високий ступінь захисту при невеликих витратах на шифрування.

Алгоритм Rivest Shamir Adleman (RSA) асиметричний. Перевагою його є те, що він працює при різній довжині ключа. Чим довше ключ, тим більше часу потрібно для розшифровки і тим вище рівень безпеки. Алгоритм шифрування реалізується програмно або апаратно.

Проблему захисту від вірусів доцільно розглядати в загальному контексті проблеми захисту інформації від несанкціонованого доступу, дотримуючись при цьому три важливих обставини.

1) Захист інформації від несанкціонованих дій ефективна тільки тоді, коли комплекцію застосовуються.

2) Захист повинна здійснюватися безперервно.

3) На захист інформації не потрібно жаліти витрат грошових, матеріальних, тимчасових і інших ресурсів, так як він багаторазово окупиться збереженням цілісності інформації.

3.2 Засоби технічного захисту мережі

Зазвичай для побудови коплексного захисту інформації використовується не одне технічне рішення, зазвичай це цілий комплекс рішень. В наступному розділі будуть приведені методи для захисту мереж, які можуть працювати як і самостійно так і співпрацювати одна з одною.

Сьогодні, діяльність будь-якої компанії багато в чому залежить від мережі Internet і тих сервісів, які вона надає, тому питання про доцільність використання Internet виникає дуже рідко. У той же час дуже гостро ставиться питання про те, щоб була можливість використовувати всі привілеї і вигоди мережі Internet з мінімальним ризиком для діяльності підприємства. Тому сьогодні на перший план виходить проблема забезпечення безпеки в комп’ютерних інформаційних системах з боку мережевого впливу.

І цей сегмент не стоїть на місці і постійно розвивається, причому дуже динамічно. Основними засобами захисту комп’ютерних ІС були, є і залишаються

міжмережеві екрани (МЕ) [5]. У літературі можна зустріти їх синоніми такі як: брандмауер, фільтруючий маршрутизатор тощо. Всі ці терміни мають на увазі одне й те саме, мають одне функціональне призначення, але можуть містити в собі різний набір інструментів захисту. МЕ є лише інструментом системи безпеки. Вони надають певний рівень захисту і є засобом реалізації політики безпеки на мережевому рівні. Рівень безпеки, який надає мережевий екран, може варіюватися в залежності від вимог безпеки.

Існує традиційний компроміс між безпекою, простотою використання, вартістю, складністю і т.д. МЕ є одним з декількох механізмів, використовуваних для управління і спостереження за доступом до і з мережі з метою її захисту.

Система міжмережевого екрану замінює маршрутизатор або зовнішній шлюз мережі. Захищена частина мережі розміщується за ним. Пакети, адресовані брандмауером, обробляються локально, а не просто переадресовуються. Пакети ж, які адресовані об'єктам, розташованим за брандмауером, не доставляються. З цієї причини хакер змушений мати справу з системою захисту брандмауера.

Така схема простіше і надійніше, так як слід дбати про захист однієї машини, а не багатьох. Найчастіше МЕ представляє з себе мережеву станцію з двома і більше мережевими інтерфейсами. При цьому через один інтерфейс здійснюється зв'язок з Інтернет, а через другий – з захищеною мережею. МЕ поєднує функції маршрутизатора-шлюзу, екрану і управління екраном.

Застосування міжмережевих екранів Firewall реалізує основні функції:

- багаторівнева фільтрація мережевого трафіку;
- перехоплює запити на інформацію і приховує адреси дійсного розміщення інформації;
- створення приватних мереж з віртуальними IP-адресами для приховування істинної топології внутрішньої IP- мережі.

Всі міжмережеві екрани функціонують на основі інформації, одержуваної від різних рівнів еталонної моделі ISO / OSI, і чим вище OSI, на основі якого побудований міжмережевий екран, тим вище рівень захисту їм забезпечується. Існують три основні типи міжмережевих екранів – брандмауер, пакетний фільтр, який працює на сеансовому рівні і шлюз на прикладному рівні.

Пакетні фільтри перешкоджають проходженню через них певних типів пакетів. Наприклад, пакетний фільтр може пропускати пакети електронної пошти, але блокувати передачу файлів.

Шлюзи канального рівня працюють за більш гнучкою схемою, ніж пакетні фільтри. Так само як і пакетні фільтри, шлюзи канального рівня можуть перешкоджати проходженню певних типів пакетів через брандмауер, але крім цього шлюз канального рівня видаляє заголовок і закінчення пакету, що прийшов і замінює їх заголовком і закінченням прийнятим з іншого боку брандмауера. Таким чином, за допомогою шлюзів канального рівня можна підключати приватні IP-мережі до Інтернету, не змінюючи адресацію приватної мережі під стандарти Інтернету.

Шлюзи додатків надають найбільшу безпеку, так як з одного боку брандмауера і з іншого ніколи насправді не спілкуються один з одним. Зовнішня станція відправляє повідомлення шлюзу додатків, який перетворює його і передає за адресою призначення з іншого боку брандмауера. На відміну від використання пакетних фільтрів або шлюзів канального рівня, обидва комп'ютера сприймають такий брандмауер як кінцеву точку мережевого потоку даних.

Зазвичай міжмережеві екрани поєднують в собі функції двох або трьох типів [5].

В даний час є нова технологія побудови міжмережевих екранів, що об'єднує в собі позитивні властивості всіх трьох типів.

Ця технологія була названа Statefue Inspection, а міжмережеві екрани відносяться до категорії Statefue Inspection Firewall.

Міжмережеві екрани володіють наступними недоліками:

- практично жоден міжмережевий екран не має вбудованих механізмів захисту від вірусів;
- зниження продуктивності мережі.

Таким чином, міжмережеві екрани є необхідними, але не достатніми засобами забезпечення інформаційної безпеки. Вони забезпечують в основному першу лінію оборони, і слід застосовувати їх спільно з іншими засобами забезпечення інформаційної безпеки.

Недоліки брандмауеру походять від її переваг, ускладнюючи доступ ззовні, система робить важким і доступ назовні. Для багатьох програм, які працюють на нестандартних портах і не підтримують проксі-сервера, для установки з'єднання доведеться або відкривати порти, або відмовитися від їх використання. Також МЕ можна використовувати разом з віртуальними приватними мережами (VPN).

Міжмережеві екрани нового покоління (NGFW) – захисне програмне забезпечення, яке включає в себе функції традиційних фаєрволів і розширені функції: більш глибоку інспекцію трафіку і проактивний систему виявлення загроз [5].

NGFW допомагає компаніям захищати мережі, пристрої та додатки від шкідливих атак, в тому числі від розвинених стійких загроз, вразливостей нульового дня, шкідливого ПЗ, програм-вимагачів і незахищеного доступу.

Експерти визначають принципову відмінність міжмережевих екранів нового покоління як здатність інспектувати і контролювати трафік за межами зв'язку «порт - протокол», тобто на рівні додатків всередині мережі. Також до вимог додалися запобігання та виявлення вторгнень, наявність засобів глибокої перевірки пакетів, оцінка репутації сайтів і розпізнавання контенту, форматів даних і користувачів.

Першою архітектурної проблемою UTM було те, що всі двигуни всередині по черзі передавали один одному мережеві пакети і чекали коли попередній движок закінчить роботу, щоб почати свою. В результаті чим більше функцій вбудовує вендор в свій пристрій, тим повільніше воно працює. В результаті користувачам таких пристроїв доводиться відключати IPS і антивірус або частина їх сигнатур, щоб трафік взагалі ходив. Тобто начебто платили як за пристрій захисту, а користуються тільки як роутером. Потрібно було щось придумати, щоб движки захисту не чекали один одного і працювали паралельно.

Новим ходом виробників NGFW стало те, що в них використовували спеціалізовані чіпи, які одночасно дивляться на той же самий трафік. Це стало можливим, оскільки кожен процесор став відповідати за свою функцію: в один прошиті сигнатури IPS, в інший сигнатури антивіруса, в третій сигнатури URL. Можна включати всі сигнатури в усіх двигунах - трафік знаходиться під повним захистом без зниження продуктивності.

Другий архітектурної проблемою UTM стало те, що всі файлові операції вимагали роботи жорсткого диска.

У сучасних UTM на цей випадок вбудовані різні механізми автоотключения роботи двигунів захисту: antivirus-bypass, ips-bypass і інші, які вимикають функції безпеки, коли завантаження апаратної частини перевищить її можливості. Тому UTM в основному застосовуються в маленьких компаніях, де швидкості були неважливі, або де безпека - опція.

Система організації захищеного віддаленого доступу користувачів до ресурсів корпоративної мережі надає можливість створення захищених Інтернет-каналів, реалізованих на базі технології побудови віртуальних приватних мереж, що забезпечує високий рівень безпеки корпоративного трафіку при невеликих фінансових витратах.

Проксі-сервер – служба (комплекс програм) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб [6]. Спочатку клієнт підключається до проксі-сервера і запитує який-небудь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного серверу і отримує ресурс у нього, або повертає ресурс із власного кешу (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінений проксі-сервером в певних цілях. Також проксі-сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак і допомагає зберігати анонімність клієнта. Найчастіше проксі-сервери застосовуються для наступних цілей.

1) Забезпечення доступу з комп'ютерів локальної мережі в Інтернет.

2) Кешування даних, тобто якщо часто відбуваються звернення до одних і тих же зовнішніх ресурсів, то можна тримати їх копію на проксі-сервері і видавати за запитом, знижуючи тим самим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації.

3) Стиснення даних, мається на увазі, що проксі-сервер завантажує інформацію з Інтернету і передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі-сервери використовуються в основному з метою економії зовнішнього мережевого трафіку клієнта або внутрішнього - компанії, в якій встановлений проксі-сервер.

4) Захист локальної мережі від зовнішнього доступу, наприклад, можна налаштувати проксі-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони «бачать» тільки проксі-сервер).

5) Обмеження доступу з локальної мережі до зовнішньої, наприклад, можна заборонити доступ до певних веб-сайтів, обмежити використання інтернету якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу і віруси.

6) Анонімізація доступу до різних ресурсів. Проксі-сервер може приховувати відомості про джерело запиту або користувача. В такому випадку цільової сервер бачить лише інформацію про проксі-сервер, наприклад, IP-адреса, але не має можливості визначити дійсне джерело запиту. Існують також проксі-сервери, які передають цільовому серверу неправдиву інформацію про користувача.

Проксі-сервери популярні серед користувачів країн, де доступ до деяких ресурсів обмежений законодавчо і фільтрується. Проксі-сервер, до якого може отримати доступ будь-який користувач мережі інтернет, називається відкритим. Проксі сервери поділяються на прозорі та зворотні.

Прозорий проксі – схема зв'язку, при якій трафік, або його частина, перенаправляється на проксі-сервер неявно (засобами маршрутизатора). При цьому клієнт може використовувати всі переваги проксі-сервера без додаткових налаштувань браузера (або іншої програми для роботи з інтернет).

Зворотний проксі – проксі-сервер, який на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або кілька серверів, логічно розташованих у внутрішній мережі. Часто використовується для балансування мережного навантаження між декількома веб-серверами і підвищення їх безпеки, граючи при цьому роль брандмауера на прикладному рівні.

Засоби антивірусного захисту призначені для перевірки файлів і пам'яті комп'ютера на наявність відомих та нових шкідливих програм, лікування заражених об'єктів і видалення загроз [6]. На рис. 3.1 зображені види антивірусних програм.

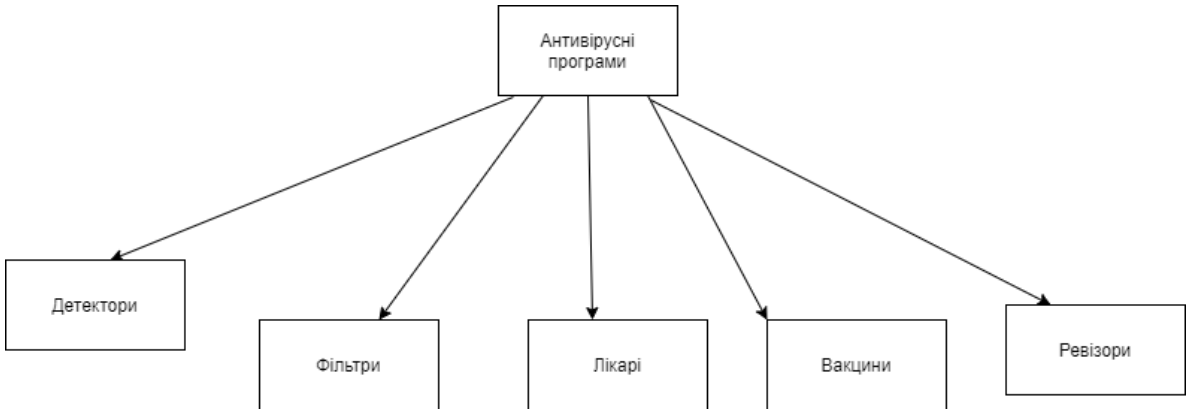

Рисунок 3.1 – Види антивірусних програм

Програми-детектори здійснюють пошук характерної для конкретного вірусу послідовності байтів в оперативній пам'яті та у файлах і при виявленні видають відповідне повідомлення. Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розробникам таких програм.

Програми-доктори або фаги, а також програми-вакцини не тільки знаходять заражені вірусами файли, але і "лікують" їх, тобто видаляють з файлу тіло програми вірусу, повертаючи файли в початковий стан.

На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх, і тільки потім переходять до "лікуванню" файлів. Серед фагів виділяють полифаги, тобто програми-доктори, призначені для пошуку і знищення великої кількості вірусів.

З огляду на, що постійно з'являються нові віруси, програми-детектори і програми-доктори швидко застарівають, і потрібно регулярне оновлення їх версій.

Програма-ревізори відносяться до найнадійніших засобів захисту від вірусів. Ревізори запам'ятовують початковий стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан з вихідним. Виявлені зміни виводяться на екран відеомонітора.

Як правило, порівняння станів проводять відразу після завантаження операційної системи. При порівнянні перевіряються довжина файла, код циклічного контролю (контрольна сума файла), дата і час модифікації, інші параметри. Програми-ревізори мають достатньо розвинені алгоритми, виявляють стелс-віруси і можуть навіть відрізнити зміни версії програми від змін, внесених вірусом.

Програми-фільтри представляють собою невеликі резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних для вірусів. Такими діями можуть бути:

- спроби корекції файлів з розширеннями COM і EXE;
- зміна атрибутів файлів;
- пряма запис на диск по абсолютному адресою;
- запис в завантажувальні сектори диска;
- завантаження резидентної програми.

При спробі будь-якої програми здійснити зазначені дії "сторож" посилає користувачеві повідомлення н пропонує заборонити або дозволити відповідну дію.

Програми-фільтри вельми корисні, оскільки здатні виявити вірус на ранній стадії його існування до розмноження. Однак вони не «лікують» файли і диски. Для знищення вірусів потрібно застосувати інші програми, наприклад фаги. До недоліків програм-сторожів можна віднести їх "настирливість" (наприклад, вони постійно видають попередження про будь-яку спробу копіювання виконуваного файлу), а також можливі конфлікти з іншим програмним забезпеченням. Прикладом програми-фільтра є програма Vsafe, що входить до складу пакету утиліт операційної системи MS DOS.

Вакцини або іммунізатори – це резидентні програми, що запобігають зараженню файлів. Вакцини застосовують, якщо відсутні програми-доктори, та цей вірус. Вакцинація можлива тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їх роботі, а вірус буде сприймати їх зараженими і тому не впровадити. В даний час програми-вакцини мають обмежене застосування.

Своєчасне виявлення заражених вірусами файлів і дисків, повне знищення виявлених вірусів на кожному комп'ютері дозволяють уникнути поширення вірусної епідемії на інші комп'ютери.

Поштовий сервер – це програма, яка передає повідомлення від одного комп'ютера до іншого [7]. Для відправки та отримання листів використовуються певні протоколи:

- SMTP, він відправляє лист поштового сервера;
- POP3, приймає лист від поштового сервера і передає одержувачу;
- IMAP, як і POP3, витягує лист з поштового сервера, але цей протокол більш сучасний і зручний.

Основна відмінність в тому, що IMAP працює з поштою безпосередньо на сервері, а POP3 скачує вхідні листи з сервера і зберігає їх локально. На рис.3.2 представлена схема відправки повідомленя від одного користувача до іншого.

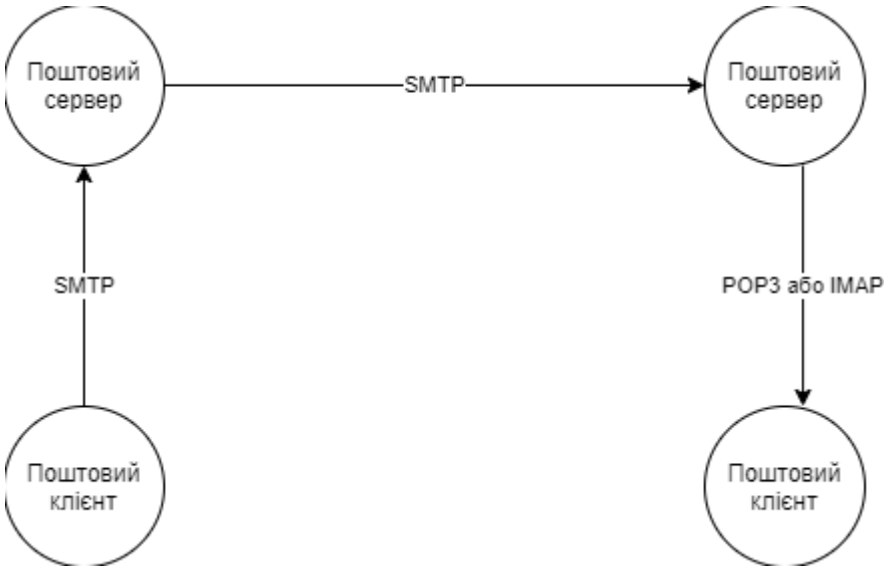

Рисунок 3.2 – Схема відправки повідомленя від одного користувача до іншого

Створити свій поштовий сервер для розсилки і збору пошти – не єдине рішення. Організувати корпоративну пошту можна і іншими способами. Вибір способу залежить від масштабів компанії, його спрямованості і бюджету, який ви готові виділити на обслуговування пошти. Нижче розглянуті способи організації корпоративної пошти.

1) Безкоштовний e-mail, зареєстрований в загальнодоступному поштовому сервісі [7]. Такий електронною поштою ми зазвичай користуємося в повсякденному житті: для особистого листування, підписки на розсилки, реєстрації в різних сервісах і т.д. Плюсами даного методу – простий і функуціональний інтерфейс, безкоштовне користування сервісом та відсутність налаштування ресурних записів. До мінусів можна віднести обмежену поштову квоту, складність підкреслити бренд компанії та небезпеку при звільнені співробітника або втратою ним поштової скриньки.

2) Пошта на домені. Ви можете зареєструвати домен, співзвучний назві вашої компанії, і використовувати його для створення поштових скриньок в будь-якому сервісі, який надає послугу пошти на домені [7]. Так, ім'я поштової скриньки буде закінчуватися назвою компанії, а починатися з чого завгодно: з назви відділу, прізвища та імені співробітника і т.д. Плюси данного методу – більшість сервісів надає послугу пошти безкоштовно підприємство оплачує тільки обслуговування домену, також компанія отримує додатковий функціонал для поштової скриньки такий, як антиспам, переадресація, тощо. До мінусів можна віднести відсутність можливості тонкого налаштування сервера під вимоги

компанії, а також при виникненні збоїв в роботі сервера неможливо вплинути на їх усунення.

3) Свій поштовий сервер. Це як пошта для домену, яка описана в попередньому пункті, тільки розширена версія є можливість налуштування не тільки домену, а й сам серверу. Плюси данного методу – гнучке налаштування сервера під потреби компанії, наприклад, можливість налаштування резервного копіювання, обмеження доступу, білі і чорні списки тощо. Також можна віднести моніторинг роботи серверу і доступ до його логів, якщо узагальнити вище сказане то компанія може контролювати роботу та надійність сервера. Що стосується мінусів, то це безумовно матеріальні витрати на покупку або оренду необхідного обладнання, також для оптимальної роботи свого серверу потрібен фахівець з навичками адміністрування Linux або Windows Server.

Система виявлення вторгнень може забезпечувати як захист конкретного вузла, так і цілого мережевого сегмента. Дана система дозволяє виявляти атаки і зловживання щодо вузлів корпоративної мережі компанії. Основний принцип роботи системи виявлення та запобігання вторгнень полягає у виявленні та блокуванні мережевих атак в корпоративної мережі на основі аналізу пакетів даних, що циркулюють в цій мережі, і в подальшому виявленні аномалій мережевого трафіку мережі. Система дозволяє з рівним ступенем ефективності виявляти і блокувати атаки з боку як зовнішніх, так і внутрішніх порушників.

Для виявлення вторгнень система використовує метод, заснований на виявленні сигнатур відомих атак, а також метод, який базується на аналізі поведінки мережі. Метод, заснований на виявленні сигнатур, забезпечує виявлення атак за допомогою спеціальних шаблонів. Як сигнатури атаки можуть виступати рядок символів, семантичне вираження на спеціальній мові, формальна математична модель та ін., Причому кожна сигнатура може бути співвіднесена з відповідною атакою порушника. При отриманні вихідних даних про трафік мережі корпоративної мережі система проводить їх аналіз на відповідність певним шаблоном або сигнатурам атак, що зберігається в постійно оновлюється базі даних системи. У разі виявлення сигнатури в вихідних даних система фіксує факт виявлення мережевої атаки і блокує її подальші дії. Перевагою сигнатурного методу є його висока точність [7].

Для виявлення нових типів атак в системі виявлення вторгнень реалізований метод, який заснований на аналізі поведінки корпоративної мережі і використовує

інформацію про штатний процесі функціонування корпоративної мережі. Принцип роботи цього методу полягає у виявленні невідповідності між поточним режимом функціонування корпоративної мережі і моделлю штатного режиму роботи, закладеної в параметрах роботи методу. Будь-яка невідповідність розглядається як інформаційна атака. У разі здійснення атаки, яка може привести до виведення з ладу вузлів корпоративної мережі, можливі автоматичне завершення з'єднання з атакуючим вузлом, блокування облікового запису порушника (якщо він є співробітником компанії) або реконфігурація міжмережевих екранів і маршрутизаторів таким чином, щоб в подальшому з'єднання з атакуючим вузлом були заборонені [7].

До складу системи виявлення та запобігання вторгнень входять наступні компоненти: мережеві сенсори, серверні сенсори, датчики, сервер управління сенсорами, а також консоль адміністратора. Мережеві сенсори, призначені для захисту об'єктів мережевих сегментів корпоративної мережі, забезпечують перехоплення і аналіз всього мережевого трафіку, що передається в рамках того сегмента, де вони встановлені. Серверні сенсори встановлюються на сервери корпоративної мережі і забезпечують захист певних мережевих сервісів мережі. У числі таких сенсорів можуть бути серверні сенсори для поштових, файлових і Web-серверів, а також для серверів баз даних. На одному сервері корпоративної мережі може бути одночасно встановлено декілька типів сенсорів. Датчики виконують функції управління серверними і мережевими сенсорами, а також функції забезпечення передачі інформації між сенсорами і сервером управління сенсорами. Сервер управління сенсорами забезпечує централізований збір, зберігання і аналіз інформації, що надходить від серверних і мережевих сенсорів, і дає можливість виявлення розподілених мережевих атак на основі аналізу отриманої інформації. Консоль адміністратора призначена для централізованого управління компонентами системи і відображення результатів роботи системи.

Повідомлення про виявлену атаці, як правило, формується відповідно до стандарту Intrusion Detection Message Exchange Format (IDMEF) і містить наступну інформацію:

- дата і час виявлення атаки;
- загальний опис атаки, включаючи можливі посилання на додаткові джерела інформації про виявлену атаці;

- символьний ідентифікатор атаки за класифікатором CVE або Computer Emergency Response Team (CERT);
- рівень пріоритету виявленої атаки (низький, середній або високий);
- інформація про джерело атаки (IP-адреса, номер порту, доменне ім'я);
- інформація про об'єкт атаки (IP-адреса, номер порту, доменне ім'я);
- рекомендації щодо усунення вразливості, в результаті якої був зафіксований факт реалізації атаки.

База даних сигнатур атак системи виявлення та запобігання вторгнень повинна регулярно оновлюватися.

При виявленні вразливостей система надає адміністратору звіти, що містять докладний опис кожної виявленої уразливості, дані про їх розташування в вузлах корпоративної мережі і рекомендації по їх корекції або усунення [7].

До складу системи аналізу захищеності входять сканери безпеки, призначені для проведення заданої множини перевірок відповідно до параметрів, визначених адміністратором безпеки; сервер зберігання результатів роботи системи; консоль адміністратора для централізованого управління системою.

Сканер безпеки являє собою програмний засіб для віддаленої або локальної діагностики різних елементів мережі на предмет виявлення в них вразливостей, використання яких може привести до комп'ютерних порушень. Основними користувачами таких сканерів є системні адміністратори і фахівці з безпеки. Сканери безпеки скорочують час, необхідний для пошуку вразливостей, за рахунок автоматизації операцій по оцінці захищеності систем. Принципи роботи такого сканера полягає в тому, що основний модуль програми приєднується по мережі до віддаленого комп'ютера. Залежно від активних сервісів формуються перевірки і тести. Знайдена при скануванні кожного порту службова інформація порівнюється з таблицею правил визначення мережевих пристроїв, операційних систем і можливих вразливостей. На основі проведеного порівняння робиться висновок про наявність чи відсутність потенційної уразливості.

Система аналізу захищеності вимагає постійної уваги і контролю [7]. Будь-яка зміна конфігурації корпоративної мережі компанії, а також мережевого програмного забезпечення має бути досліджено системою аналізу захищеності. Невідповідність в конфігурації може привести до збільшення кількості помилкових спрацьовувань, а також до появи дірок в безпеці. Робота системи заснована на аналізі мережевого трафіку з використанням методу сигнатур, тому

система аналізу захищеності вимагає постійного оновлення бази вразливостей. Експлуатація даної системи має сенс тільки за умови, що вона розвивається разом з мережею, яку вона захищає. Зрозуміло, що мається на увазі регулярне проведення тестів.

В даний час багато компаній, що займаються питаннями інформаційної. Пропонують стратегію застосування описаних вище систем в складі єдиних комплексів, що дозволяють здійснювати централізоване управління інформаційною безпекою корпоративної мережі. За допомогою єдиного управління всіма компонентами підсистеми інформаційної безпеки корпоративної мережі, а також на основі збору і аналізу інформації від різних компонентів в режимі реального часу можна значно підвищити ефективність роботи адміністраторів безпеки, скоротити число співробітників відповідних служб і зменшити витрати на їхнє навчання.

Подібні системи дозволяють вести єдину базу даних шаблонів, варіантів реагування і оновлень для всіх компонентів підсистеми безпеки, автоматизувати рутинні завдання адміністраторів безпеки (оновлення сигнатур атак, сканування віддалених вузлів і т.д.), а також проводити всебічний аналіз різних подій шляхом кореляції даних від різноманітних засобів захисту.

Багато користувачів вважають, що для забезпечення надійного захисту цілком достатньо антивірусного програмного забезпечення, інші вважають, що краще рішення це повна шифрація даних. Однак використання антивірусного ПЗ при його правильному налаштуванні і експлуатації означає всього лише те, що віруси із загальновідомих списків з великою часткою ймовірності не потраплять в захищається інформаційний ресурс. Крім того, існує велика кількість програм, типу троянців і т.п., які не виявляються антивірусним програмним забезпеченням і можуть функціонувати на зараженому комп'ютері роками. Повне шифрування даних саме по собі теж не є панацеєю, так як шифрована стійкими алгоритмами важлива інформація може бути легко передана зловмисникові так званими клавіатурними шпигунами. У той же час слід враховувати, що система шифрування є одним з ключових елементів єдиної комплексної підсистеми інформаційної безпеки корпоративної мережі компанії.

Virtual Private Network (VPN) – це приватна віртуальна мережа. Підключення до такої мережі відбувається поверх вашого звичайного з'єднання з інтернетом. Це означає, що для підключення до VPN-мережі потрібно мати

функціональне з'єднання з інтернетом. Основна відмінність між VPN і звичайним підключенням полягає в шифруванні. Всі дані, передані по VPN, піддаються шифрування і по ідеї недоступні для перегляду третім особам.

Засоби захисту як підключення до VPN, так і передачі даних різні і можуть сильно відрізнятися у постачальників послуг. За своєю суттю VPN діляться на два типи:

- віддалений доступ – підключення комп'ютера до мережі;
- site-to-site – з'єднання двох різних мереж.

Корпоративні VPN-мережі, як правило, використовуються для віддаленого доступу співробітників до внутрішніх ресурсів компанії через зашифроване з'єднання. Site-to-site VPN в даному випадку служить для того, щоб співробітники, що знаходяться в різних мережах, могли після підключення працювати всередині однієї загальної віртуальної мережі.

Існує ще третій варіант: Client-Server VPN. Такий спосіб з'єднання служить, коли сервера потрібно створити і надати клієнтам кілька різних мереж. Таким чином, користувачі всередині однієї мережі підключаються до сервера і передають йому дані по двом різним внутрішнім мережам. Якщо говорити більш точно, то VPN можна класифікувати за такими параметрами:

- за ступенем захищеності використовуваного середовища;
- за способом реалізації (програмне рішення або інтегроване);
- за призначенням;
- за типом протоколу;
- за доступом (платно, безкоштовно).

Тунель це підключення між вашим комп'ютером і комп'ютером-сервером. Обидва комп'ютера, в свою чергу, називаються вузлами. Кожен з вузлів відповідає за ступінь захищеності з'єднання до того, як вони потраплять в тунель.

VPN-з'єднання завжди складається з каналу типу «точка-точка», також відомого під назвою «тунель». Тунель створюється в незахищеній мережі, в якості якої найчастіше виступає Інтернет. З'єднання «точка-точка» має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються вузлами. Кожен вузол відповідає за шифрування даних до того, як вони потраплять в тунель, і розшифровка цих даних відбудеться після того, як вони покинуть тунель.

Після підключення до VPN-сервера всі дані починають передаватися між комп’ютером і сервером в зашифрованому вигляді. Уже з VPN-сервера всі дані передаються до зовнішніх ресурсів, які запитуються.

Варто врахувати, що на практиці далеко не вся передана інформація шифрується. При виборі VPN-провайдера слід врахувати кілька важливих параметрів:

- ступінь шифрування з'єднання;
- приховування факту підключення до сервера;
- зберігання логів;
- співпраця при видачі інформації третім особам.

Багато VPN-провайдерів гарантують повну відсутність логів, а значить, при видачі інформації третім особам їм просто не буде чого дати. Також рівень шифрування у багатьох провайдерів приблизно однаковий.

Другий важливий момент це приховування факту підключення до сервера. Більш рідкісна послуга у VPN-провайдерів. Справа в тому, що при підключенні до сервера або різкому роз'єднання ваш провайдер може отримати частину даних, які були передані. Тому деякі розробники пропонують захист від витоків при підключенні це технологія Multihop VPN. У цьому випадку з'єднання з сайтом відбувається через кілька VPN-серверів. На рис. 3.3 зображена схема з’єдання користувача з Інтернетом з VPN та без нього.

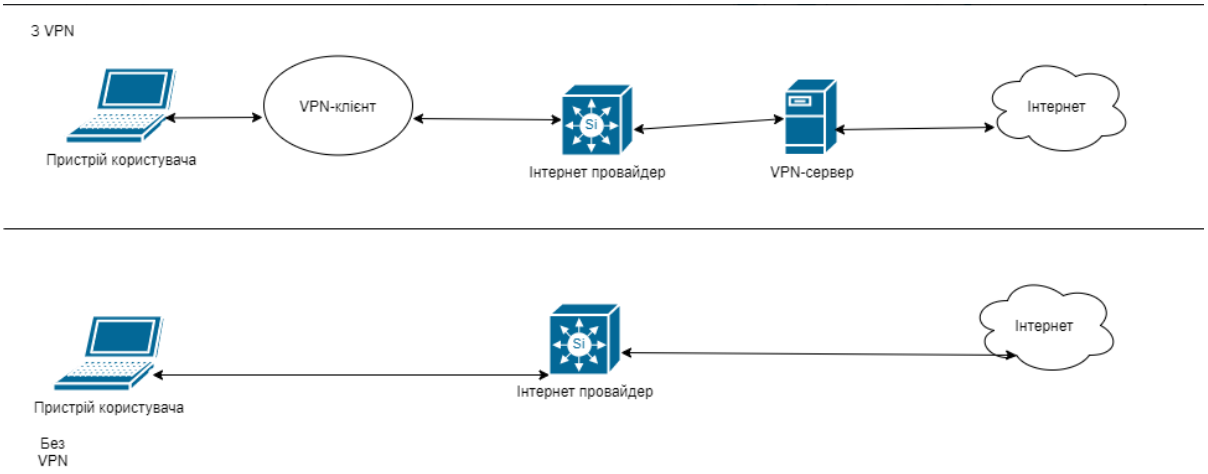

Рисунок 3.3 – Схема роботи VPN

До недоліків VPN можна віднести відносну складність розгортання, додаткові витрати на ключі аутентифікації і збільшення пропускної здатності інтернет каналу. Ключі аутентифікації також можуть бути скомпрометовані.

Вкрадені мобільні пристрої компанії або співробітників (ноутбуки, планшети, смартфони) з попередньо налаштованими параметрами підключення VPN можуть стати потенційною діркою для несанкціонованого доступу до ресурсів компанії.

3.3 Система управління політикою безпеки і захисту від несанкціонованого доступу

Перш за все слід зазначити, що дана система не виконує функцій захисту від таких зловмисних дій, як використання побічних електромагнітних випромінювань і наведень, підслуховування, підглядання і т.п. Для протидії подібного роду порушень повинен бути реалізований комплекс організаційно-технічних заходів по фізичній контролю (розміщення, охорона і т.п.) контрольованих вузлів корпоративної мережі [9]. Основний же завданням системи управління політикою безпеки і захисту від несанкціонованого доступу є виявлення фактів несанкціонованих дій користувачів корпоративної мережі на основі збору і аналізу інформації про події, що реєструються на інформаційних ресурсах корпоративної мережі.

Дана система забезпечує моніторинг, контроль і збір інформації про дії легальних користувачів корпоративної мережі. Якщо за результатами аналізу зібраних даних виявляється факт несанкціонованих дій, система блокує подальші дії порушника і оповіщає адміністратора безпеки про дії користувача. Крім того, система контролює роботу додатків, запущених на робочих станціях користувачів. Інформація про випадок порушення політики безпеки записується в базу даних системи і може використовуватися для подальшого аналізу.

У завдання цієї системи входить збір інформації про наступні події:

- зміна файлової системи контрольованого вузла корпоративної мережі;
- використання зовнішніх пристроїв введення-виведення (дисководів, USB-пристроїв і т.п.);
- запуск і зупинка процесів на контрольованому вузлі;
- локальна або віддалена реєстрація початку сеансу роботи користувача, а також завершення роботи користувачів;
- використання принтерів і інших периферійних пристроїв;
- ведення статистики використання мережевих сервісів;
- зміна апаратної й програмної конфігурації контрольованого вузла.

Система управління політикою безпеки і захисту від несанкціонованого доступу має розподілену архітектуру і включає такі компоненти, як програмні сенсори, сервер управління сенсорами і консоль адміністратора. Програмні сенсори встановлюються на контрольовані вузли корпоративної мережі і забезпечують збір, фільтрацію і передачу параметрів зібраних подій сервера управління сенсорами. Сервер управління сенсорами здійснює зберігання і аналіз інформації про події, що надходять від сенсорів системи [9]. Консоль адміністратора служить для централізованого управління сервером управління сенсорами і сенсорами системи, відображення результатів роботи системи і формування звітів.

Політика зокрема повинна включати:

- стратегію захисту IT-інфраструктури організації;
- набір правил, за якими створюється, обробляється і зберігається інформація на підприємстві;
- правила своєчасного оновлення ПЗ і відповідальність працівників;
- створення резервних копій та відновлення даних.

Необхідно регулярно створювати резервні копії бізнес-систем і критично важливих даних. Резервні копії повинні зберігатися на окремих носіях інформації, які фізично відокремлені від цільових систем. Цілісність і повнота резервних копій повинна регулярно перевірятися шляхом штатного відновлення. Правила використання облікових записів в організації, повинні включати наступні твердження.

1) Персоніфікований адміністративний доступ. Заборона на використання загальних адміністративних облікових записів.

2) Використання різних облікових записів для виконання різних адміністративних завдань, таких як, адміністрування домену, адмініструвння серверів, адміністрування ПК користувачів та адміністрування власного ПК.

3) Заборона здійснювати регулярні завдання по використанню адміністративних облікових записів. Адміністратори повинні працювати на своїх ПК під стандартними обліковими записами з правами рівня звичайного користувача. Робота з адміністрування інформаційних систем повинна здійснюватися з окремого виділеного термінального сервера управління (або спеціалізованих систем PAM, а не безпосередньо з призначеного для користувача ПК [9]. Використання адміністратором для певних робіт відповідного облікового

запису має суворо контролюватися. Заборона використання облікових записів адміністраторів домену для завдань, не пов'язаних з адмініструванням контролерів доменів. Гранулярна деталізація прав доступу сервісних облікових записів. Облікові записи для функціонування різних служб і ПО повинні мати мінімально необхідний рівень прав, достатній для роботи конкретного сервісу. Дотримання принципу максимально повної персоніфікації: кожне ПО може використовувати окремий акаунт.

4) Регулярне навчання всіх користувачів організації основам інформаційної безпеки, що включає в себе донесення правл роботи з критичними системами організації та донесення правил роботи з інформацією, що надходить із зовнішніх неперевірених джерел. До цього також можна віднести проведення регулярного зрізу знань для контролю засвоєння інформації співробітниками.

5) Регулярне навчання та підвищення кваліфікації фахівців у галузі інформаційних та адміністраторів в області сучасних загроз і методів захисту на системах і рішеннях, які експлуатуються в організації.

6) Проведення тестових атак, в тому числі з використанням методів «соціальної інженерії», для перевірки обізнаності Користувачів в правилах безпеки організації і рівні захищеності інформаційних систем.

Засоби управління політикою безпеки і захисту від несанкціонованого доступу реалізують комплексні рішення для організації доступу користувачів і адміністраторів до ресурсів корпоративної мережі, передбачають використання електронних ключів з унікальними персональними ідентифікаторами користувачів, електронних замків та інших засобів захисту серверів, робочих станцій і телекомунікаційного устаткування від несанкціонованого доступу.

Адміністратору підсистеми безпеки слід мати на увазі те, що конфіденційна інформація компанії може бути послана співробітником компанії по електронній пошті. Для виявлення подібних фактів підсистема безпеки повинна включати засоби контролю вмісту поштових повідомлень.

А тепер буде більш детально розглянуто системи управління політикою безпеки і захисту від несанкціонованого доступу, засоби виявлення і запобігання вторгнень, а також інструменти аналізу захищеності ресурсів корпоративної мережі.

3.4 Рекомендації щодо побудови захищеної мережі підприємства

Для того щоб побудувати захищену мережу насамперед впроваджують контроль на периметрі корпоративної мережі. Для контролю переметру використовують мережні екрани з функціями контролю на прикладному рівні і системи протидії вторгнень (ips) – next generation firewall (ngfw) [9]. Також необхідно розташувати публічні сервіси в окремих нейтральних зонах, а також налаштувати конкретизовані правила доступу для контролю потоків даних і відмова від використання загальних сутностей типу «any», «all».

Також для захисту периметру необхідно використовувати проксі сервер для контролю доступу користувачів організації до мережі інтернет, ще необхідно встановити блокування доступу до ресурсів із забороненою тематикою, поганою репутацією, високим рівнем ризику, фішингових ресурсів. Обов'язковим пунктом є – виконання антивірусної перевірки і контентної фільтрації завантаження. У тому числі потрібно блокувати завантаження виконуваних файлів для загальної групи користувачів. Крім того необхідно налаштувати повної інспекції ssl для виявлення загроз в зашифрованому трафіку Відповідно потрібно організувати заборону використання безумовних білих списків доступу до зовнішніх ресурсів і організувати білі списки внутрішніх систем в обхід правил тематичної перевірки [9].

У тому числі для створення захищеного периметру необхідно використовувати поштовий шлюз для захисту корпоративної пошти від спаму та зовнішніх загроз. Потрібно налаштувати для вхідних листів антивірусну перевірку і зробити правила фільтрації контенту по типу файлів та їх розширення. Блокувати листи або одразу видаляти листи з вкладеннями виконувальних файлів або офісних документів з макросами. Перевіряти всі посилання в листі на належність до небезпечних і заборонених сайтів, з високим ступенем ризику і фішингу.

Передавати інформацію між сегментами компанії і при віддаленому доступі користувачів через інтернет-канали зв'язок повинен здійснюватися тільки за допомогою VPN з використанням належного рівня шифрування (aes-256 і вище), а також з обов'язковим моніторингом і фіксацією виконаних дій.Також все вищезначене стосується, як зовнішніх партнерів так і підрядників компанії.

Однак недостатньо зробити лише захищений периметр мережі, ще потрібно організувати безпеку всередині самої мережі. Наступні рекомендації будуть відноситися до контролю мережі [10].

Насамперед потрібно сегментувати локальну мережу згідно функціонального призначення, тобто поділити сервіси на відповідні серверні сегменти. Також необхідно заборонити створення сегментів з великою кількістю систем, оскільки VLAN технологія допускає створення сегменту з 4096 пристроями. Для особливо критичних систем і сервісів потрібно провести мікросегментацію мережі, тобто в ідеалі розміщати по принципу один сегмент-одна система.

Також потрібно ізолювати порти на комутаторах доступу користувачів для заборони прямої взаємодії між призначеними для користувача системама.

Аналогічним чином потрібно налаштувати технології протидії атакам типу ARP-спуфінг і dhcp-серверів для запобігання перехоплення трафіку [10].

Також необхідно блокувати пряму мережну взаємодію між інтернет-сервісами і корпоративною мережею. Зв'язок між сегментами потрібно здійснювати тільки через проксі-сервери, розташовані в нейтральних зонах на стику мереж. До того ж трафік між нейтральною зоною і інтернет-ресурсами, а також між нетральною зоною і корпоративною мережею потрібно контролювати за допомогою міжмережевих екранів.

Наступним кроком буде підвищення захищеності систем, експлуатованих в організації (мережних пристроїв, серверних і призначених для користувача систем) для зменшення поверхні можливої атаки на мережу. До рішень можна віднести нижчезазначене [10].

Для початку потрібно видалити і відключити зайві компоненти і служби, які не використовуються і не потрібні в робочому процесі. Також потрібно відмовитись від використання застарілих протоколів таких як NTML, SMBv1 тощо. Потрібно впровадити механізми і заходи з протидії отримання паролів з пам’яті і системних процесів.

До того ж потрібно заборонити створення локальних облікових записів або зміни їх паролів доменними політиками, оскільки інформація про акаунт і його пароль доступні всім користувачам мережі. У тому числі До вище сказаного також можна віднести регулярне оновлення системного і прикладного програмного забезпечення. Необхідно забезпечити своєчасне тестування і

оперативне встановлення оновлень безпеки для системного і прикладного програмного забезпечення з урахуванням рівня критичності і пріоритетів. Також потрібно ввімкнути блокування механізму автоматичного визначення проксі-серверів WPAD.

Також необхідно постійно перевіряти наявність встановленого актуального антивірусного програмного забезпечення на серверних і вашій системі організації. Регулярне оновлення антивірусних компонентів і баз даних сигнатур. Заборона можливості рядовим користувачам локально змінювати конфігурацію антивірусного ПО і вимикати модулі. До того ж організувати Наявність на системах організації встановленого рішення Host IPS з активованим функціоналом:

- мережного екрану з налаштованими мінімально необхідними для роботи дозвільними правилами;
- сигнатурної захисту від атак, як на мережевому рівні, так і в рамках самої системи;
- блокування втручання невідомих процесів в роботу і системну пам'ять інших;
- поведінковий аналіз дій програмного забезпечення процесів і блокування в разі підозрілої активності;
- блокування дочірніх процесів, які породжують офісні документи.

Крім того необхідна наявність функціоналу контролю запуску додатків і програм, що включає можливість:

- створення списків дозволеного програмного забезпечення на робочій станції;
- перевірку репутації виконуваних файлів в хмарі;
- контроль поновлення тільки перевіреними програмами, з довірених джерел, авторизованими користувачами.

До того ж всього вищесказаного необхідна наявність рішення для контролю підключення периферійних пристроїв і знімних носіїв до робочих станцій організації. Також налаштувати правила для вирішення підключення тільки перевірених корпоративних носіїв [10].

Коли всі вищеперечислені рекомендації були зроблені для впровадження ще більшь високого рівня захисту можна впровадити рішення 802.1x і network access control (nac) для запобігання несанкціонованого підключення сторонніх пристроїв

в корпоративну мережу і забезпечення надання тільки необхідної мережевого доступу в залежності від функціональних обов'язків користувача і стану пристрою. Данне рішення забезпечить:

- контроль пристроїв, що підключаються до корпоративної мережі. блокування сторонніх пристроїв;
- гранульований доступ в мережу за результатами авторизації (політика доступу в залежності від користувача, часу, способу, місця підключення і типу пристрою);
- можливість реалізувати попередню перевірку пристроїв на відповідність перед підключенням до корпоративної мережі (nac): наявність встановленого антивіруса і інших продуктів, актуальність останніх оновлень.

Також можна впровадити спеціалізований засіб «пісочниці» (sandbox) для статичного (аналіз коду) і динамічного (запуск в тестовому середовищі) аналізу невідомих файлів на предмет виявлення їх шкідливих дій. Для підвищення ефективності антивірусного захисту в протидії атакам типу «zero-day» рішення sandbox необхідно інтегрувати з максимальною кількістю систем захисту: мережевими екранами веб та поштовими шлюзами, засобами захисту на кінцевих системах. Також системи цього класу можуть використовуватися адміністраторами, як додатковий інструмент у дослідженні загроз.

Крім того можна використати системи контролю дій привілейованих користувачів – privilege access management (pam). Це рішення надає доступ до критичних систем, забезпечуючи:

- збір, запис і аналіз активності привілейованих користувачів;
- детектування ризикованих дій до того, як це призведе до шкідливих наслідків;
- можливість взаємодії з користувачем, який виконує ризиковані операції, і блокування сесії.

Аналогічним чином можна налаштувати системи моніторингу та профілювання мережевих потоків для визначення штатного профілю трафіку організації і виявлення відхилень від «нормального» поведінки. налаштування збору інформації про трафік з усіх ключових мережевих пристроїв організації для повноти видимості і аналізу потоків даних [10].

Плюсом до всього буде наявність спеціалізованого рішення vulnerability assessment для регулярного сканування всіх елементів корпоративної

інфраструктури на предмет виявлення відомих вразливостей в операційних системах і ПЗ. Забезпечення можливості оперативного усунення виявлених загроз і виконання інтеграції з системами мережевої безпеки і аналітики для ізоляції або фільтрування доступу до вузлів з критичними уразливими.

Також можна використовувати системи централізованого збору, аналізу та кореляції подій безпеки (siem) для всебічного комплексного аналізу стану корпоративної інфраструктури, що забезпечує наступні переваги.

1) Збір журнальної інформації та подій з усіх систем підприємства приведення отриманих подій до єдиного вигляду (нормалізація) і агрегація даних.

2) Створення екранів і звітів для відображення стану іт-інфраструктури.

3) Створення правил кореляції для виявлення пов'язаних подій, які можуть свідчити про атаки і спроби компрометації в іт-інфраструктурі організації.

4) Створення правил кореляції на основі ризиків для виявлення і виділення небезпечних дій і подій, що відбуваються на критичних системах.

5) Аналіз історичних даних для створення нових правил кореляції.

6) Налаштування правил для автоматичної реакції на виявлені події з метою в максимально короткі терміни блокувати і припинити поширення загроз.

4 ПОЕТАПНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

В даному розділі перераховані процедури, які сприяють побудові системі інформаційного захисту компанії, або при її наявності, підвищення рівня безпеки на підприємстві. Також перераховані інструменти, які будь-який SMB може використати для підвищення свого рівня інформаційної безпеки.

4.1 Поетапний підхід до побудови системи захисту інформації

Данна методика пропонує використовувати поетапний підхід до побудови системи захисту інформації. Етапи побудови розписані нижче.

1) Перший етап дозволяє зрозуміти, що знаходиться у мережі, і визначає базові вимоги щодо інформаційної безпеки.

2) Другий етап приділяє основну увагу забезпеченню базових вимог безпеки і навчання співробітників питань інформаційної безпеки.

3) Третій етап допомагає вашій організації підготуватися до інцидентів з інформаційної безпеки.

На самому початку, щоб просунутися в питанні інформаційної безпеки, необхідно розібратися з локальною мережею, підключеними пристроями, критично важливими даними та програмами. Без чіткого розуміння того, що потрібно захищати, важко зрозуміти чи відповідає створена система безпекі вимогам. Постановка задачі на даному етапі зводиться до наступного:

- вирішити, яку інформацію необхідно захищати;
- вирішити, де в мережі компанії зберігається найважливіша інформація;
- отримання списку пристроїв підключених до мережі компанії;
- отримання списку ПЗ встановленого на комп’ютерах співробітників;
- провести опитування серед системних адміністраторів та користувачів, щодо надійності їх паролів;
- моніторинг онлайн-ресурсів, які відвідують співробітники.

Витік критично важливих даних, їх викрадення або пошкодження можуть привести до тимчасової зупинки роботи підприємства або навіть до його

банкрутства. Випадкові події та природні катаклізми також потенційно можуть завдати непоправної шкоди.

Крім того, потенційні зловмисники націлені на дані, які можуть мати цінність для них. Цими зловмисниками можуть бути як хакери, так і співробітники компанії, які хочуть переманити клієнтів компанії собі або викрасти фінансову інформацію чи інтелектуальну власність. Щоб використовувати цінну інформацію, вони повинні отримати до неї доступ, а доступ, як правило, вони отримують через локальну мережу організації.

Щоб захистити інформаційну безпеку компанії, потрібно розуміти цінність даних компанії і як їх можна використовувати. Також необхідно визначити, яку інформацію потрібно захищати в рамках законодавства, наприклад, платіжна інформація або персональні дані. Нижче представлені приклади даних, які необхідно ідентифікувати і інвентаризувати:

- кредитні карти, банківська та фінансова інформація;
- персональні дані;
- бази даних клієнтів;
- ціни на закупівлю / поставку;
- комерційні секрети компанії;
- формули, методології, моделі, інтелектуальна власність.

Якщо відомо які пристрої підключені до мережі, то інфраструктура стає простіше в управлінні, і приходить розуміння, які пристрої необхідно захищати.

Нижче описані дії, які ви необхідно зробити, щоб дізнатися про пристрої у мережі підприємства.

1) Якщо мається бездротова мережа, потрібно перевірити на маршрутизаторі (контролері бездротового доступу) які пристрої підключені, і чи застосовується надійне шифрування (WPA2).

2) Для більших організацій пропонується застосування мережевого сканера для ідентифікації всіх пристроїв у мережі.

3) Ввімкнення логування подій, пов'язаних з підключенням мережевих пристроїв, які отримують ip-адреса по протоколу DHCP. Логування таких подій забезпечить зручне відстеження всіх пристроїв, які були у мережі.

4) У невеликих організаціях можна зберігати список обладнання. І перелік інформації, що захищається в електронній таблиці, яку необхідно оновлювати при появі нового обладнання або даних.

Для реалізації перерахованих цілей, добре підійдуть наступні інструменти:

- Nmap;
- ZenMap;
- Spiceworks.

Контроль встановленого програмного забезпечення є ключовим компонентом як доброго врядування ІТ, так і ефективного захисту інформації. Шкідливе програмне забезпечення у мережі може створювати ризики, які необхідно мінімізувати, сюди ж можна віднести юридичну відповідальність за використання неліцензійного програмного забезпечення.

Неоновлення програмне забезпечення є поширеною причиною іншим шкідливим яке призводить до атак на ваші інформаційні системи. Коли є розуміння, яке програмне забезпечення встановлено у мережі, є контроль за ПЗ, яке буде встановлене і є захист облікових записів з правами адміністратора, то це вже кардинально зменшує імовірність і вплив інцидентів інформаційної безпеки.

Нижче наведені описані дії, які потрібно виконати, контролювати програмне забезпечення компанії.

1) Створення переліку додатків, веб-сервісів або хмарних рішень, які використовує компанія.

2) Обмеження числа користувачів з правами адміністратора до мінімально можливого значення. Заборонити звичайним користувачам працювати в системі з правами адміністратора.

3) Використовувати складні паролі для адміністративних облікових записів, так як адміністратори можуть вносити серйозні зміни в систему. Розробити інструкцію для співробітників зі складання складних паролів.

4) Переконатися, що системні адміністратори використовують окрему призначену для користувача обліковий запис для читання електронної пошти, доступу в Інтернет і складання документів.

5) Розробка процедури встановлення програмного забезпечення в мережі.

Для реалізації перерахованих цілей, добре підійдуть наступні інструменти:

- Applocker;
- Netwrix;
- OpenAudIT.

На другому етапі проектування необхідно замислитись про захист активів компанії. Співробітники – це один з найважливіший актив, зв'язку з чим потрібно з повною відповідальністю поставитися до захисту співробітників. Захист інформації вимагає не тільки технологічних рішень, а й обізнаності співробітників про запобігання випадкового порушення роботи систем компанії.

В рамках цього етапу не тільки буде описана захист комп'ютерів або пристроїв в мережі, а також навчання ваших співробітників важливим аспектам інформаційної безпеки. Цей етап зводиться до наступних цілей:

- налаштування пристроїв в мережі з урахуванням вимог інформаційної безпеки;
- налаштування регулярних оновлень антивірусного ПЗ;
- проведення брифінгів на тему сучасних методів захисти інформації для співробітників.

Для отримання доступу в інформаційну систему шкідливі програми і зловмисники найчастіше використовують або небезпечно налаштовані додатки, до яких ПЗ є вразливим. Необхідно переконатися, що операційна система і додатки (особливо веб-браузери) оновлені і правильно налаштовані. Крім того, рекомендується використовувати механізми захисту від шкідливих програм, які можуть бути вбудовані в вашу операційну систему.

Нижче наведені описані дії, які потрібно виконати, контролювати оновлення ПЗ в компанії.

1) Періодичний запуск сканеру безпеки Microsoft Security Analyzer, щоб визначити, які оновлення не встановлені для операційної системи Windows, і які зміни в конфігурації необхідно виконати.

2) Визначити, що браузер і плагіни в ньому оновлені.

3) Використання антивірусу з останніми оновленнями антивірусної бази для захисту систем від шкідливого ПЗ.

4) Обмеження використання знімних носіїв (USB, CD, DVD) тими співробітниками, кому це дійсно потрібно для виконання своїх службових обов'язків.

5) Вимога щодо використання багатофакторної аутентифікації там, де це можливо, особливо для віддаленого доступу до внутрішньої мережі або електронною поштою. Наприклад, використання безпечних токенів, смарт-карт

або смс повідомлення з кодами в якості додаткового рівня безпеки на додаток до паролів.

6) Зміна паролів за замовчуванням для всіх додатків, операційних систем, маршрутизаторів, міжмережевих екранів, точок бездротового доступу, принтерів, сканерів і інших пристроїв, при додаванні їх в мережу.

7) Шифрування жорстких дисків на ноутбуці або мобільному пристрої, що містять конфіденційну інформацію.

Для реалізації перерахованих цілей, добре підійдуть наступні інструменти:

- Bitlocker;
- FireVault;
- Qualys Browser Check;
- OpenVAS;
- Microsoft Baseline Security Analyzer;
- CIS Benchmarks.

Стосуючись інформаційної безпеки, можна сказати, що не тільки технології ,а ще і процеси в ній та дії людей. Недостатньо наявності тільки засобів захисту інформації. Щоб забезпечити безпеку компанії, співробітники також повинні суворо дотримуватися вимог з інформаційної безпеки. Є два ключові чинники для навчання співробітників питань інформаційної безпеки: донести інформацію до них, постійно підтримувати їх рівень знань. Інформація, яку необхідно донести до співробітників.

1) Визначити співробітників, які мають доступ або обробляють конфіденційну інформації, і переконатися, що вони розуміють свою роль в захисті цієї інформації.

2) Двома найпоширенішими атаками є фішингові атаки по електронній пошті і по телефону. Переконатися, що співробітники можуть описати і визначити основні ознаки атаки. До таких ознак можуть відноситися ситуації, коли люди просять цінну або конфіденційну інформацію, використовують незрозумілі або технічні терміни, просять ігнорувати або обійти процедури безпеки.

3) Заохочувати використання складних, унікальних паролів для кожного облікового запису і (або) двухфакторну аутентифікацію там, де це можливо.

4) Вимагати від співбітників використовувати блокування екрану на своїх пристроях.

5) Переконатися, що всі співробітники постійно оновлюють свої пристрої і ПЗ на них.

Недостатньо одного разу провести тренінг по інформаційній безпеці, потрібно ще ці знання підтримувати у співробітників. Для цього по-перше потрібно пояснювати співробітникам, як захистити інтереси компанії і як ці методи можна застосувати в особистому житті. Також потрібно обов'язково переконатися, що вони розуміють, що інформаційна безпека є важливою частиною роботи. Потрібно поширювати серед співробітників обов'язкові для проходження інформаційні матеріали з питань інформаційної безпеки, або використовувати онлайн ресурси з інформаційної безпеки.

Для реалізації перерахованих цілей, добре підійдуть наступні інструменти:

- SANS Ouch!;
- MS-ISAC;
- Staysafeonline.com.

Після того, як компанія розробила серйозний фундамент з інформаційної безпеки, треба вибудувати механізми реакції на інциденти. Такий підхід включає в себе розуміння, як справлятися з інцидентом інформаційної безпеки і як відновити роботу компанії після нього.

Цей етап буде описувати наступні задачі:

- регулярна перевірка наяності резервних копій;
- регулярна перевірка правильності резервних копій;
- визначення відповідального співробітника, який буде реагувати на інцидент безпеки.

Створення та управління резервними – це один з кращих способів захистити дані, відновитися після збою і повернути компанію в робочий режим. Це важливо, тому що програми-вимагачі можуть зашифрувати всі дані і заблокувати їх до викупу. Надійний план реагування, доповнений поточними і підтримуваними резервними копіями, є найкращим захистом при роботі з інцидентом з інформаційної безпеки.

Нижче наведені описані дії, які потрібно виконати, щодо резервоного копіюваня в компанії.

1) Автоматично виконувати щотижневі резервні копії всіх комп'ютерів, що містять важливу інформацію.

2) Періодично перевіряти резервні копії, відновлюючи систему з використанням резервної копії.

3) Переконатися, що, хоча б одна резервна копія недоступна по мережі. Це допоможе захистити від атак програм-вимагачів, оскільки дана резервна копія не буде доступна для шкідливого ПЗ.

Для реалізації перерахованих цілей, добре підійдуть наступні інструменти:

- Microsoft «Створення резервної копії та відновлення»;
- Apple Time Machine;
- Amanda Network Backup;
- Bacula.

Ніяк і ніхто не може спрогнозувати, коли відбудеть інцидент безпеки, але чим краще компанія підготовлена, тим швидше вона зможе відновитися після інциденту. До інцидентів з інформаційної безпеки відносять атаку типу відмова в обслуговуванні, яка порушує доступ до вашого сайту, атаку програм-вимагачів, які блокують вашу систему або ваші дані, атаку шкідливим ПЗ, яка призводить до втрати даних вашого клієнта або співробітника, а також крадіжку ноутбука, що містить незашифровані дані.

Щоб бути готовим, потрібно знати, до кого звернутися в разі інциденту. Можна звернутися до внутрішнього IT-персоналу за допомогою, або до сторонньої сертифікованої компанія, яка надає послуги з управління інцидентами. У будь-якому випадку, потрібно знати відповідальних за управління інцидентами до виникнення події.

В першу чергу, керівник відділу інформаційної безпеки має визначитись із поняттям інцидент інформаційної безпеки. Це допоможе встановити межі відповідальності відділу та класифікувати інциденти за пріоритетами їх критичності. Єдиного поняття терміну інцидент інформаційної безпеки немає, але описати його можна через супутні складові – це подія, яка відповідає наступним вимогам:

- здійснена особою або групою осіб;
- використано комп’ютерні ресурси;
- потенційно/реально несе шкоду інформаційно-комунікаційній системі.

Ніхто не застрахований від того, що під визначення «інцідент інформаційної безпеки» можуть потрапити події, які, насправді, ними не

являються. І до певного часу не можна бути певними, чи маєте ви справу з інцидентом, чи з подією.

4.2 Розробка плану реагування на інцидент

Наступним кроком буде розробка плану реагування на інцидент і формування команди реагування.

Відповідно, план повинен бути чітким і зрозумілим для всіх, а команда реагування повинна бути постійно готовою, тому найкраще, якщо це буде включено до їхніх посадових обов'язків [11]. Отже, потрібно почати з плану реагування на інцидент. Процес обробки інциденту зображено на рис. 4.1.

Рисунок 4.1 – Процес обробки інциденту

Система моніторингу виявляє проблему. Після цього запускається процес інформування керівника команди реагування. Він, у свою чергу, ініціює План реагування та підключає Команду реагування. Під час роботи команди важливо документувати увесь хід розслідування.

По-перше, це знадобиться для майбутньої оцінки ефективності команди реагування.

По-друге, якщо компанію притягнуть до відповідальності, документація послужить доказовою базою того, що ви вжили відповідних мір для розв'язання інциденту, та/або інцидент стався не через вашу вину.

Після закінчення процесу розв'язання інциденту запускається процес оцінки ефективності Команди реагування. Головна мета оцінки ефективності, як у класичних підходах проектного менеджменту – це визначити слабкі місця у роботі команди реагування і розробити відповідні заходи, щоб зробити її більш ефективною [11].

Отже, покроковий організайційний план реагування на інциденти інформаційної безпеки представлений нижче.

1) Визначення інциденту інформаційної безпеки.

2) Класифікація інцидентів ІБ за ступенем ризику.

3) Згідно класифікації розробка максимально чіткого та зрозумілого плану реагування на інцидент.

4) Створення команди реагування і ознайомлення її з планом реагування.

5) Постійна оцінка ефективності роботи цієї схеми та її вдосконалення.

6) Ведення документації по всіх проведеним розслідуванням.

В результаті компанія отримає відповідність ряду нормативних та організаційних вимог. Зокрема, доказову базу у разі виявлення несанкціонованого доступу до даних згідно GDPR, а також відповідність вимогам розділу №4 Постанови №95 НБУ.

Щодо організаційних переваг, то у довгостроковому терміні компанія отримає економію фінансових, людських і часових ресурсів, а також зниження ризиків матеріальних та нематеріальних втрат від кіберінцидентів.

5 МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ КОМПАНІЇ

IT-компанія – це офісне приміщення з великою кількістю компьютерного обладнання, такого як: комп’ютери, сервери, маршрутизатори тощо. Зокрема в роботі буде розглянута абстрактна IT-компанія «ООО».

Складається вона з двоповерхової будівлі та автостоянки для персонального автотранспорту співробітників компанії, розміщених на єдиній території оточеній парканом. Також компанія має два територіально розділених філіали.

Фізична безпека корпоративної мережі є одним з найважливіших факторів, який складно переоцінити. Маючи фізичний доступ до мережних пристроїв зловмисник, в більшості випадків, легко отримає доступ до вашої мережі. Наприклад, якщо є фізичний доступ до комутатора і в мережі не проводиться фільтрація MAC-адрес. Хоча і фільтрація MAC в цьому випадку вас не врятує. Ще однією проблемою є крадіжка або недбале ставлення до жорстких дисків після заміни в сервері або іншому пристрої

Фізична охорона забезпечується цілодобово в робочий час в кількості двох співробітників охорони (один на прохідній другий в офісній будівлі). У вихідні та неробочі години фізична охорона забезпечується одним співробітником. У цілодобовому режимі функціонують системи пожежної, тривожної сигналізації, відеоспостереження. На рис. 5.1 зображено топологію мережі компанії до введення засобів захисту.

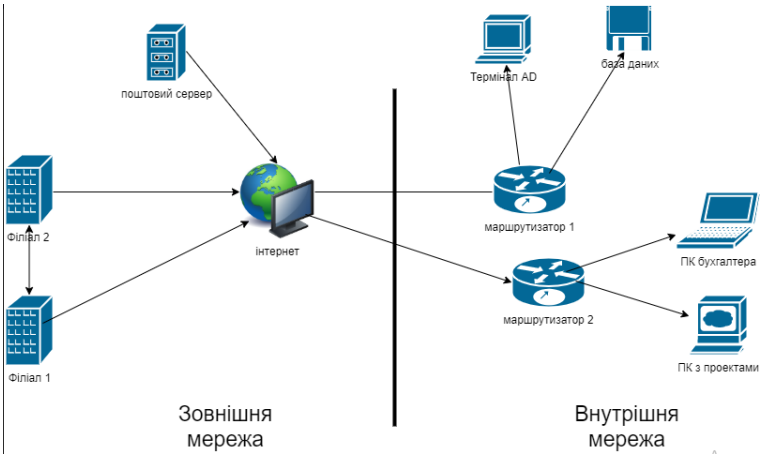

Рисунок 5.1 – Топологія мережі до введення захисту

Метод визначення ймовірності порушення критичних властивостей ІА був застосований на практиці. За допомогою системи контролю захищеності MaxPatrol було проведено сканування чотирьох вузлів, що входять до складу однієї корпоративної мережі. На данних хостах було виявленно 193 вразливості. На основі даних про ці вразливості були визначені імовірності порушеня критичних властивостей, зв'язаних з реалізацією вразливостей ПЗ хостів. У таблиці 5.1 зображено імовірності порушеня критичних властивостей зв'язаних з реалізацією вразливостей ПЗ хостів.

Таблиця 5.1 – Вірогідність порушення критичних властивостей в результаті використання вразливостей програмного забезпечення хостів

Програмне забезпечення	Критична властивість	IP-адреса хоста			
		192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4
MS SQL	К	0,84	-	-	-
	Ц	0,84	-	-	-
	Д	0,84	-	-	-
MS Windows server	К	-	0,51	-	-
	Ц	-	0,51	-	-
	Д	-	0,51	-	-
MS Windows	К	-	-	0,82	0,813
	Ц	-	-	0,8	0,796
	Д	-	-	0,71	0,602

У таблиці 5.2 зображені вірогідності порушеня порушення критичних властвостей в результаті використання вразливостей хостів.

Таблиця 5.2 – Вірогідність порушення критичних властивостей в результаті використання вразливостей хостів

Критична властивість	IP-адреса хоста			
	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4
К	0,99	0,93	0,95	0,902
Ц	0,89	0,887	0,96	0,913
Д	0,85	0,8	0,91	0,94

У таблиці 5.3 зображені вірогідності порушення критичних властивостей інформаційних активів.

Таблиця 5.3 – Вірогідність порушення критичних властивостей інформаційних активів

Інформаційний актив	IP-адреса хоста	Імовірність порушення критичних властивостей		
		К	Ц	Д
Облікові записи користувачів	192.168.1.2	0,66	0,66	0,6
Проектна документація	192.168.1.3	0,275	0,66	0,6
Бухгалтерський облік	192.168.1.4	0,66	0,66	0,6

Виходячи з рекомендацій з другого розділу для організації захисту зовнішнього периметру мережі був використані наступні програмні та апаратні рішення.

Спочатку була використана система виявлення вторгнень та системи протидії атакам. На сьогоднішній день у багатьох системах використовується функціонал IPS, але найчастіше ці функції або усічені, або для їх виконання виділяється дуже мало ресурсів. Тому для данної цілі був вибраний програмний продукт McAfee® Host Intrusion Prevention для серверів. Це програмне рішення, яке здійснює захист як від відомих, так і невідомих погроз нульового дня, DDoS-атак, SSL-атак і прихованих загроз об'єднуючи запобігання вторгнення на основі аналізу поведінки і сигнатур з фаєрволом і контролем додатків, що забезпечує безперебійну роботу сервера і захищає корпоративні активи, такі як додатки і бази даних. Після впровадження рішення архітектура мережі набула наступного вигляду.

Далі було вирішено поставити зворотній проксі – сервер. Зворотний проксі-сервер дозволяє розміщувати за фаєрволом кілька веб-вузлів і веб-серверів одночасно, і при цьому використовувати єдиний маршрутизації IP-адреса. IPS (система запобігання вторгнень) і система фільтрації антивірусної програми працюють зі зворотним проксі-сервером.

Було вирішено використовувати зворотний проксі, а не звичайний, бо зворотній проксі – є єдиною точкою входу для будь-якого веб-сайту або файлового сервера, розміщеного за фаєрволом. Це дає наступні переваги.

1) Підвищену безпеку – серверна топологія і мережеві характеристики заховані від зовнішнього світу.

2) Спрощену аутентифікацію – єдина точка аутентифікації для всіх сервісів, розташованих за фаєрволом.

3) Просте управління SSL-сертифікатами веб-сайтів, розміщених з використанням HTTPS, тобто відпадає необхідність у сертифікатах для кожного веб-сервера, знижуючи навантаження на веб-сервера при шифруванні.

Було вирішено використовувати програмний пакет Kerio Control.

Далі був поставленний та налаштований апаратний міжмережний екран. Було вирішено встановити фаєрвол фірми Barracuda.

Така топологія мережі є правильно оскільки саме такий порядок розташування захисту в мережі дозволяє профільтрувати всі надходячі загрози.

Після попередніх дій було вирішено поставити свій поштовий сервер, оскільки він передбачає найбільш гнучке налаштування спам фільтрів.

Далі було вирішено використати віртуальні приватні мережі, оскільки компанія має два територіально розділених підрозділи та також частина співробітників працюють не з офісу, а дистанційно. Для данного рішення був використанний програмний продукт NordVPN, один із найпопулярніших продуктів на ринку.

Також було встановлено антивірусне ПЗ на клієнтські пристрої та робочі станції. Бізнес-версії антивірусів включають функції централізованого управління для передачі оновлень антивірусних баз клієнтські пристрої, а також можливість централізованої настройки політики безпеки. В асортименті антивірусних компаній присутні спеціалізовані рішення для серверів.

Перший підхід передбачає, що в операційній системі за замовчуванням дозволено запуск будь-яких додатків, якщо вони раніше не внесені до "чорного списку".

Другий підхід, навпаки, передбачає, що дозволений запуск тільки тих програм, які заздалегідь були внесені до білого списку, а всі інші програми за замовчуванням блокуються. Другий підхід до безпеки звичайно більш кращий в корпоративному світі. Білі списки можна створити, як за допомогою вбудованих

засобів операційної системи, так і за допомогою стороннього ПО. Антивірусне ПЗ часто пропонує дану функцію в своєму складі. Більшість антивірусних програм, що пропонують фільтрацію по білому списку, дозволяють провести первинне налаштування дуже швидко, з мінімальним увагою з боку користувача.

Проте, можуть виникнути ситуації, в яких залежно файлів програми з білого списку були правильно визначені вами або антивірусним ПЗ. Це призведе до збоїв програми або до неправильної його установки. Крім того, білі списки безсилі проти атак, що використовують уразливості обробки документів програмами з білого списку.

Після впровадження мір захисту ситуація з безпекою змінилася в кращу сторону. Програмою MaxPatrol було виявлено вже не 193 вразливості, а 54, що наводить на думку, що відбулося посилення мір захисту в компанії. На рис. 5.2 зображена топологія мережі після впровадження мір захисту.

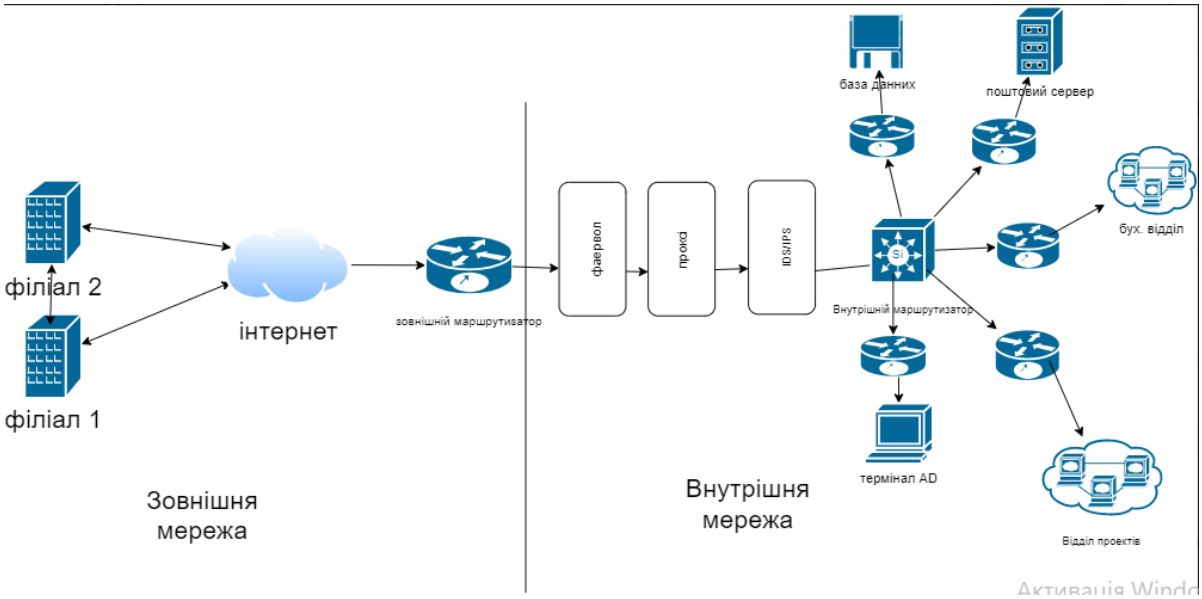

Рисунок 5.2 – Топологія мережі після впровадження мір захисту

У таблиці 5.4 зображено вірогідність порушення критичних властивостей в результаті використання вразливостей програмного забезпечення після впровадження захисту, значення якої наводять на думку, що впровадженні засоби безпеки спрацювали.

Таблиця 5.4 – Вірогідність порушення критичних властивостей в результаті використання вразливостей програмного забезпечення після впровадження захисту

Програмне забезпечення	Критична властивість	IP-адреса хоста			
		192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.4
MS SQL	К	0,273	-	-	-
	Ц	0,212	-	-	-
	Д	0,273	-	-	-
MS Windows server	К	-	0,19	-	-
	Ц	-	0,21	-	-
	Д	-	0,19	-	-
MS Windows	К	-	-	0,314	0,323
	Ц	-	-	0,32	0,318
	Д	-	-	0,3	0,31

У таблиці 5.5 зображені вірогідності порушення критичних властивостей інформаційних активів після впровадження мір захисту.

Таблиця 5.5 – Вірогідність порушення критичних властивостей інформаційних активів після впровадження захисту

Інформаційний актив	IP-адреса хоста	Імовірність порушення критичних властивостей		
		К	Ц	Д
База данних	192.168.1.1	0,132	0,132	0,055
Облікові записи користувачів	192.168.1.2	0,264	0,264	0,264
Проектна документація	192.168.1.3	0,055	0,528	0,055
Бухгалтерський облік	192.168.1.4	0,132	0,528	0,66

ВИСНОВКИ

В атестаційній роботі було вирішена задача щодо аналізу та класифікації загроз в комп’ютерних мережах. Також була досліджена методика загальної оцінки вразливостей CVSS. Крім того були досліджені методи захисту комп’ютерних мереж та були надані рекомендації щодо їх впровадження в комп’ютерну мережу. Було встановлено, що існуючі методики захисту погано себе показують поодинці і для побудови якісної системи захисту повинен використовуватися комплес рішень. Також був описаний підхід до проектування системи безпеки ІТ компанії та був запропонований план дій при інцидентах безпеки. Враховуючи переваги та недоліки засобів захисту мережі та наведених рекомендацій щодо побудови комплексного захисту мережі була змодельована система захисту мережі. Після цього за допомогою математичного апарату теорії ймовірностей, були вираховані ймовірності порушення критичних властивостей для інформаційних активів мережі.

Був проведений порівняльний аналіз локальної мережі компанії до впровадження мір захисту і після. Показано, що запропонована система інформаційної безпеки має місце бути оскільки показники імовірності порушення критичних властивостей інформаційних активів знизились.

Окремі результати роботи опубліковані у [12 – 14].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Структура локальної мережі підриємства [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.sviaz-expo.ru/ru/articles/struktura-lokalnoj-seti-predpriyatiya.

2. Рекомендації інформаційної безпеки для малого та середнього бізнесу [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post 348892.

3. Мережні атаки [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html.

4. Закон України «Доступ до публічної інформації» [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/ 2939-17.

5. Terri W. O. Firewalls. Практичне застосування міжмережевих екранів / William Olgtri Terri. – Київ: ДМК Пресс, 2001. – 400 с. – (Захист та адміністрування).

6. 8 основних рубежів захисту комп’ютерних мереж [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.it-lines.ru/blogs/security/ osnovnye-metody-zashhity-korporativnoj-seti.

7. Методи захисту мереж [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://studopedia.su/6_4733_metodi-zashchiti-setey.html.

8. Росляков О. О. Віртуальні приватні мережі. Основи побудови та застосування / О. О. Росляков, С. В. Попов. – Київ: Еко-трендз, 2006. – 301 с. Snader J. J. VPNs illustrated: Tunnels, VPN’s and IPsec / John Junior Snader., 2006. – 445 с.

9. Захист мережі: комплексний підхід [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://goo.su/16VM.

10. Концепції захисту IT-інфраструктури від сучасних загроз [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://netwave.ua/ru/ kontseptsy-ya-zashhy-ty-y-t-y-nfrastruktury-ot-sovremenny-h-ugroz.

11. Чому потрібен план реагування на кіберінциденти [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://nv.ua/ukr/biz/experts/chomu-potriben-plan-reaguvannya-na-kiberincidenti-2472078.html.

12. Тертичний В.О. Використання фазової інформації мовного сигналу користувача в системах голосової автентифікації / Є.Є. Куценко, В.О. Тертичний, Р.А. Сердюк. // Одеса, ОНАЗ, Інфокомунікації – сучасність та майбутнє: тези доповідей 9-ій міжнародній науково-практичній конференції. – 2019. – С.198–200.

13. Тертичний В.О. Кібербезпека хмарних обчислень та баз даних / В.О. Тертичний, Є.Є Куценко. // Харків, ХНУРЕ, Матеріали XXIV міжнародного молодіжного форуму «Радіоелектроніка та молодь в XXI столітті». – 2020. С. 225-227;

14. Тертичний В.О. Мережна безпека, система виявлення та протидії атакам, відмовостійкість мереж / В.О. Тертичний. // Харків, ХНУРЕ, Матеріали XXIV міжнародного молодіжного форуму «Радіоелектроніка та молодь в XXI столітті». – 2020. С. 281-283.