Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістр

студента *Хіблін Миколи Миколайовича*

академічної групи *125-22м-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз та підвищення рівня захищеності інтернет-мережі підприємства «ЯВІР ДНІПРО-1»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.ф.-м.н., проф. Гусєв О.Ю.			
розділів:				
спеціальний	ас. Рибальченко Ю.П.			
економічний	к.е.н., доц. Пілова Д.П.	87	Добре	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«____»_____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістр

студенту *Хібліну Миколи Миколайовичу* **академічної групи** *125-22м-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Аналіз та підвищення рівня захищеності інтернет-мережі підприємства «ЯВІР ДНІПРО-1»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.2023 №1227-с

Розділ	Зміст	Термін виконання
Розділ 1	СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ Аналіз та дослідження інформаційної безпеки при роботі в інтернет-мережах	27.09.2023 - 06.10.2023
Розділ 2	СПЕЦІАЛЬНА ЧАСТИНА Організаційні заходи інформаційної безпеки. Впровадження систем виявлення та попередження атак інтернет-мережі	07.10.2023 - 15.11.2023
Розділ 3	ЕКОНОМІЧНИЙ РОЗДІЛ Визначення та аналіз економічної ефективності системи захисту інтернет-мережі	16.11.2023 - 24.11.2023

Завдання видано _____ Гусєв О.Ю.__
(підпис керівника) (прізвище, ініціали)

Дата видачі: 21.09.2023 р.

Дата подання до екзаменаційної комісії: 30.11.2023 р.

Прийнято до виконання _____ Хіблін М.М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 117 с., 24 рис., 13 табл., 9 додатків, 22 джерел.

Мета роботи полягає в проведенні аналізу та запропонуванні заходів щодо підвищення рівня захищеності інтернет-мережі підприємства «ЯВІР ДНІПРО-1» за допомогою програмних, апаратних і організаційних заходів.

У розділі стан питання проводиться аналіз та дослідження інформаційної безпеки при роботі в інтернет-мережах.

У спеціальній частині розглядаються організаційні заходи інформаційної безпеки, а також впровадження систем виявлення та попередження атак інтернет-мережі підприємства «ЯВІР ДНІПРО-1».

У економічному розділі наведені розрахунки та обґрунтування всіх заходів, спрямованих на вдосконалення та аналіз економічної ефективності захищеності інтернет-мережі.

Практичне значення роботи полягає в підвищенні рівня захищеності інтернет-мережі шляхом програмних, апаратних і організаційних заходів.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, МІЖМЕРЕЖЕВИЙ ЕКРАН, СИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК, ПАРОЛЬНИЙ ЗАХИСТ.

ABSTRACT

Explanatory note: 117 p., 24 fig., 13 tab., 9 additions, 22 sources.

The purpose of the work is to conduct an analysis and propose measures to increase the level of security of the Internet network of the enterprise «YAVIR DNIPRO-1» with the help of software, hardware and organizational measures.

In the state of the issue section, analysis and research of information security when working in Internet networks is carried out.

In a special part, the organizational measures of information security, as well as the implementation of systems for detecting and preventing attacks on the Internet network of the enterprise «YAVIR DNIPRO-1» are considered.

The economic section provides calculations and justification of all measures aimed at improving and analyzing the economic effectiveness of Internet network security.

The practical significance of the work consists in increasing the level of Internet network security through software, hardware and organizational measures.

INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY, THREAT MODEL, VIOLATOR MODEL, FIREWALL, ATTACK DETECTION AND PREVENTION SYSTEM, PASSWORD PROTECTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДМЗ - демілітаризована зона;

ІБ - інформаційна безпека;

ІС - інформаційна система;

КМ - комп'ютерна мережа;

ЛКМ - локальна комп'ютерна мережа;

ОІД - об'єкт інформаційної діяльності;

ПЗ - програмне забезпечення;

ПК - персональний комп'ютер;

СВВ - система виявлення вторгнень;

ТОВ - товариство з обмеженою відповідальністю;

APT - Advanced Persistent Threat, постійна серйозна загроза;

BS - British Standard, Британський стандарт;

DDoS - Distributed Denial of Service, розподілений відмова у обслуговуванні;

FTP - File Transfer Protocol, протокол передачі файлів через мережу;

HIPS - Host-based Intrusion Prevention System, система запобігання вторгненням;

IDS - Intrusion Detection System, система виявлення атак (вторгнень);

IP - Internet Protocol, протокол мережевої адресації;

ISO - International Organization for Standardization, міжнародний стандарт;

NAT - Network Address Translation, трансляція мережевих адрес;

TCP - Transmission Control Protocol, протокол керування передачею;

TIAS - Threat Intelligence Analytics System, система аналізу інтелектуальних загроз;

VPN - Virtual Private Network, віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси.

ЗМІСТ

ВСТУП

Комп'ютери, мережі та Інтернет стали невід'ємною частиною нашого повсякденного життя. Нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових відносин.

Тому стає очевидно, що для безпечної роботи такої величезної системи необхідно вживати певних заходів безпеки. Це пояснюється тим, що практично з будь-якого комп'ютера можна отримати доступ до будь-якої мережі будь-якої організації. Та важливо враховувати, що небезпека значно зростає, оскільки для злому комп'ютера не потрібний фізичний доступ.

Згідно з даними, отриманими Інститутом комп'ютерної безпеки (Computer Security Institute) в результаті нещодавно проведеного дослідження, у 70% організацій було зламано системи мережевого захисту. Крім того, 60% виявлених спроб зломів виходили з внутрішніх мереж організацій.

На сьогодні безпека інтернет-мережі стала важливою потребою для будь-якої організації. Загрози безпеці зростають із кожним днем, а високошвидкісні дротові та бездротові мережі та Інтернет-послуги стають небезпечними та ненадійними.

Актуальність теми дипломної роботи полягає в тому, що неможливо досягти необхідного рівня безпеки комп'ютерних систем і мереж без знання та компетентного застосування сучасних технологій, стандартів, протоколів і засобів забезпечення кібербезпеки.

Мета роботи полягає в проведенні аналізу та запропонуванні заходів щодо підвищенню рівня захищеності інтернет-мережі підприємства «ЯВІР ДНІПРО-1» за допомогою програмних, апаратних і організаційних заходів.

Об’єктом дослідження в роботі є інтернет-мережа «ЯВІР ДНІПРО-1».

Предметом дослідження в роботі є підвищення захищеності інтернет-мережі.

В роботі поставлені наступні завдання, пов'язані з інформаційною безпекою, яка включає комплекс заходів для забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення:

- отримання доступу до секретних або конфіденційних даних;

- порушення або повне припинення роботи комп'ютерної інформаційної системи;

- отримання доступу до керування роботою комп'ютерної інформаційної системи;

- знищення або спотворення даних.

Потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем.

Advanced persistent threat (APT) - різновид складних кібератак, спрямованих на отримання несанкціонованого доступу до інформаційних систем жертви та встановлення прихованого доступу з метою використання або контролю в майбутньому

Велика частина поточних загроз в одній чи іншій формі є ознаками APT-атак.

Отже, необхідно провести аналіз та підвищити захист інтернет-мережі завдяки впровадженню засобу, спроможного своєчасно виявити реалізацію певних загроз:

1. Реалізація загрози підвищення привілеїв;

2. Реалізація загрози підміни програмного забезпечення;

3. Реалізація загрози несанкціонованого створення обліковому запису користувача;

4. Реалізація загрози впровадження коду або даних.

ПРОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Техніко-економічна характеристика предметної галузі та підприємства

1.1.1 Загальна характеристика підприємства

Об'єктом інформаційної діяльності (ОІД) є підприємство в якій знаходиться товариство з обмеженою відповідальністю «ЯВІР ДНІПРО-1». Підприємство «ЯВІР ДНІПРО-1» було зареєстроване 30.01.2019 за юридичною адресою: 49064, Дніпропетровська обл., місто Дніпро, проспект Сергія Нігояна, будинок 22/26 в п'ятиповерховому будинку ОІД на першому поверсі (додаток Б).

Керівником організації є Афанасенко Олександр Анатолійович.

На момент останнього оновлення даних станом на 01.10.2023 статус організації не підлягає припиненню. Ситуаційний план представлений у додатку Б.

Область діяльності - охорона об'єктів (розробка, встановлення, налаштування, модернізація, обслуговування охоронних систем та їх супровід на об'єктах).

1.1.2 Організаційно-функціональна структура підприємства

Організаційна структура зображена на рис. 1.1. Голова відділу технічного забезпечення має 2 бригади, кожна з яких складається з 3 чоловік на авто компанії і виконує замовлення клієнтів.

Співробітники, які постійно працюють в головному офісі: директор, голова відділу технічного забезпечення, головний менеджер, 2 менеджера, головний бухгалтер, бухгалтер, спеціаліст з питань кібербезпеки, системний адміністратор та офісний менеджер. Загальна кількість співробітників в офісі - 10 осіб.

Так само можна віднести до штату охоронців (2 людини) і прибиральницю (1 людина), які найняті всіма фірмами, що знаходяться в будівлі.

Рисунок 1.1 - Структурна схема управління «ЯВІР ДНІПРО-1»

1.2 Методика дослідження інформаційної безпеки при роботі в інтернет-мережах

Проблема забезпечення інформаційної безпеки (ІБ) сучасних автоматизованих систем (АС) підприємства стоїть у ряді перших і найважливіших. Складність цих систем, розгалуженість тих, що становлять їх основу комп'ютерних мереж ще більше посилюють ситуацію. У теоретичному плані одним з актуальних напрямів є розробка методики оцінки ІБ на етапах проєктування, розробки і функціонування інтернет-мереж [7].

Важливість цього напряму полягає, передусім, в обґрунтуванні необхідності застосування тих або інших засобів забезпечення ІБ і способів їх використання, а також у визначенні їх достатності або недостатності для конкретної АС.

Аналіз показує, що нині існують два основні підходи до оцінки ІБ АС.

Перший на основі характеристик оцінки механізмів і достатності системи захисту. Висновок про рівень ІБ робиться на підставі значення показника ефективності системи захисту. При цьому у рамках цього підходу

увага приділяється лише одному з аспектів інформаційної безпеки, захисту інформації від несанкціонованого доступу.

Другий підхід заснований на тісному зв'язку системи показників кількісних оцінок ІБ АС з ефективністю функціонування цій АС в умовах дії усіх видів загроз ІБ. Цей підхід є методологічно вірнішим з точки зору системного аналізу, оскільки в цьому випадку виконується один з основних принципів системного підходу, який полягає в тому, що кожен елемент системи, виконуючи певну функцію, сприяє досягненню мети.

Аналіз вказує на те, що розробка методики оцінки ІБ передбачає існування або розробку моделі об'єкту оцінки, моделі системи захисту, а в деяких випадках - моделі потенційного порушника.

Наявність моделі об'єкту оцінки потрібна для визначення існуючих в ньому зв'язків, процесів, виявлення конкретних елементів, що вимагають захисту, характерних вразливостей та загроз, а також вироблення показників ІБ. Модель потенційного порушника є важливою для визначення конкретних стратегій поведінки, а також уточнення характеру загроз, що виникають від цього джерела.

Однією з найпоширеніших методик є так звана оцінка згідно з вимогами нормативних документів. В результаті задоволення тим або іншим вимогам АС відносять до того або іншого класу захищеності. Прикладом такого підходу є міжнародний стандарт ISO/IEC 15408.99, відомий як «Критерії оцінки безпеки інформаційних технологій», розроблений у рамках проєкту «Загальні критерії».

Інший підхід, базується на аналізі ризиків, передбачає оцінку ризиків, пов'язаних із загрозами безпеки щодо ресурсів АС. Відомі методики можна класифікувати за типом процедур ухвалення рішень, використовуваних в них: одноетапні, де оцінка ризиків проводиться одноразовою вирішальною процедурою, і багатоетапні, які передбачають попереднє оцінювання ключових параметрів. Одноетапні методики, як правило, використовуються на початковій стадії проєктування АС, коли ключові чинники, що визначають

інформаційну безпеку, ще не виявлені. Однак недоліком таких процедур є велика міра «суб'єктивного чинника» в оцінці ризику і труднощі їх використання для аналізу ризиків [9].

Багатоетапні методики з попереднім оцінюванням ключових параметрів вважаються більш конструктивними. Наприклад, методика оцінки ризиків, описана в спеціальних рекомендаціях 800-30 (NIST), передбачає попереднє оцінювання двох параметрів: потенційного збитку і ймовірності реалізації загрози. Проте цей метод має досить «жорсткий» механізм отримання оцінок ризиків, що суттєво обмежує його можливості. Інші відомі методики отримання оцінок ризиків з попереднім оцінюванням трьох ключових параметрів, такі як метод CRAMM. У цьому підході, окрім потенційного збитку і ймовірності реалізації загрози, оцінюється також міра вразливості АС. Можна сказати, що методика оцінювання ризиків CRAMM в порівнянні з методикою NIST є більш конструктивною, оскільки вона дозволяє аналізувати більше параметрів за точнішими шкалами. Механізм отримання оцінок ризиків, який використовується в CRAMM, залишається табличним, тобто відображає лише взаємозв'язки між рівнями, визначеними для шкал вхідних даних і величинами ризику [6].

Відомий підхід до визначення безлічі ризиків полягає в розгляді їх як декартового добутку множини загроз, безлічі вразливостей і множини активів об'єкту оцінки :

$$R = Y \cdot V \cdot A \tag{1.1}$$

Ця множина ризиків визначає множину збитків

$$U = R \cdot S \tag{1.2}$$

де S - множина цінностей активів.

На основі оцінок елементів кількостей великої кількості параметрів, пропонується ввести узагальнені та приватні інтегральні показники захищеності. В якості узагальнених інтегральних показників захищеності (ІПЗ) пропонується використати:

- середній ризик нанесення збитку власникам активів від дії усіх видів загроз без використання засобів забезпечення безпеки, що характеризує вразливість;

- середній збиток, який наноситься власникам активів при реалізації усіх видів загроз без використання засобів забезпечення безпеки.

В якості приватних інтегральних показників захищеності запропоновано використовувати:

- середній ризик нанесення збитку при реалізації загрози певного виду через усі можливі вразливості на активи усіх типів. Цей показник характеризує міру небезпеки загрози певного виду та величину збитку, пов'язаного із цією загрозою;

- середній ризик нанесення збитку від дії усіх видів загроз через усі можливі вразливості на певний тип активів. Цей показник характеризує незахищеність активів певного типу та величину збитку, пов'язаного із загрозами цього типу, і т. д.

Таким чином, питання оцінки ІБ в АС, незважаючи на існуючі нині рішення, як і раніше залишається актуальним. При усій важливості цього напряму, до теперішнього часу немає простих в описі і використанні і досить точних методик оцінки ІБ АС (під точністю потрібно розуміти, передусім, адекватність використовуваних при оцінці моделей).

Рішення завдання удосконалення методик оцінки рівня ІБ АС пов'язане з первинними умовами, які мають бути визначені в технічному завданні на АС, а також з підвищенням об'єктивності початкових даних, що використовуються при розрахунках [12].

Досягнення підвищення об'єктивності початкових даних можна здійснити кількома способами. По-перше, це може бути досягнуто через підвищення складності підходу до проблеми оцінки, яка включає розгляд заходів захисту не лише організаційного або програмно-технічного характеру, але й усіх аспектів, що піддаються деталізованій оцінці заходів захисту, включаючи фізичний захист. По-друге, підвищення об'єктивності початкових

даних можна досягти за допомогою зміни підходу до оцінювання ресурсів. Для цього в першу чергу необхідно визначити відповідний критерій оцінювання.

1.3 Аналіз ризиків підприємства

1.3.1 Ідентифікація і оцінка інформаційних активів

Одним з етапів аналізу ризиків є ідентифікація усіх об'єктів, які потребують захисту від зловмисників. Необхідно враховувати всі чинники, які можуть бути порушені при порушенні режимів безпеки.

На сучасному підприємстві в обігу перебуває величезна кількість інформації, яка охоплює всю організаційну структуру, починаючи від директора і закінчуючи продавцями, та яка тісно взаємодіє між собою. Ця взаємодія здійснюється шляхом об'єднання всієї організаційної структури в локальну обчислювальну мережу.

Комерційною таємницею називають режим конфіденційності інформації, що дозволяє її володарям, при наявних або можливих обставинах, збільшувати доход, уникати невиправданих витрат, зберігати присутність на ринках товарів, робіт, послуг або отримувати інші комерційні переваги.

Організація правильного конфіденційного діловодства в організаціях складає основну частину комплексного забезпечення безпеки даних і набуло великої важливості для досягнення їхніх цілей з захисту. За відомостями фахівців у галузі інформаційної безпеки, приблизно 80 % конфіденційних даних містяться в документах, які стосуються діловодства. Тому питання конфіденційного документообігу в організаціях, очевидно, відіграє важливу роль у досягненні комерційного успіху.

Потрапляння конфіденційної інформації до рук зловмисників і конкурентів може призводити до різних негативних наслідків для фірми, таких як збиток матеріальним активам, діяльності і престижу фірми, а також втрати стратегічно важливих замовників. Інформацію щодо оцінки активів «ЯВІР ДНІПРО-1» представлено у таблиці 1.1.

Таблиця 1.1 - Оцінка інформаційних активів підприємства

Вид діяльності	**Найменування активу**	**Форма представлення**	**Власник активу**	**Критерії визначення вартості**	**Розмірність оцінки**	
					Кількісна оцінка (од.вим.)	**Якісна**
1	2	3	4	5	6	7
Відомості ділового характеру						
Внутрішній регламент діяльності	детальні плани капітальних вкладень в розвиток підприємства	електронному виді	директор	вартість його відтворення	тис. гривень	дуже висока
	плани і методи просування послуг на ринок	електронному виді	директор	репутація компанії	тис. гривень	висока
Інформаційний актив з торговельно-економічних питань						
Обробка заявок клієнтів	Номенклатура і кількість послуг зі взаємних зобов'язань	електронному виді	менеджер	втрата доступності	тис. гривень	середня
Внутрішній регламент діяльності	Відомості про відкритих розрахункових і інших рахунках. Операції по банківських рахунках	електронному виді	головний бухгалтер	втрата доступності	тис. гривень	дуже висока
	Інформація про ефективність угод, договорів	електронному виді	директор	втрата доступності	тис. гривень	середня
	ІПН, документи про сплату податків і обов'язкові платежі	електронному виді	головний бухгалтер	втрата доступності	тис. гривень	висока

Продовження таблиці 1.1 - Оцінка інформаційних активів підприємства

1	2	3	4	5	6	7
Інформаційний актив про послуги, що надаються						
Обробка заявок клієнтів	Відомості про оброблені і необроблені замовлення	електронному виді	менеджер	вартість його відтворення	тис. гривень	середня
Внутрішній регламент діяльності	Проєкти, що розробляються, по автоматизації підприємств і бізнес-процесів	Електронному виді	директор	вартість його відтворення	тис. гривень	висока
Інформаційний актив з питань забезпечення безпеки						
Внутрішній регламент діяльності	Інформація про організацію і стан фізичної охорони адміністративної будівлі	електронному виді	директор	вартість його відтворення	тис. гривень	дуже висока
	Інформація про інформаційні ресурси, що захищаються	електронному виді	директор	втрата доступності	тис. гривень	дуже висока
	Бази даних «ЯВІР ДНІПРО-1»	електронному виді	системний адміністратор	вартість його відтворення	тис. гривень	дуже висока
	Інформація про детальну структуру корпоративної мережі	електронному виді	системний адміністратор	втрата доступності	тис. гривень	дуже висока
Інформаційний актив по організаційно-управлінській діяльності						
Внутрішній регламент діяльності	Умови індивідуальних трудових договорів з працівниками та керівниками	електронному виді	головний бухгалтер	репутація компанії	тис. гривень	середня
Товар організації						
Отримання прибутку	Комплектуючі для сигналізації	матеріальний об'єкт	директор	первинна вартість активу	тис. гривень	висока
Устаткування						
Забезпечення необхідних умов роботи	Комп'ютери, принтери, телефони, кабелі і т.д.	матеріальний об'єкт	директор	первинна вартість активу	тис. гривень	середня

На сьогодні існує більше 30 різних видів конфіденційної інформації. У загальному врахуванні це може ускладнювати створення сприятливої атмосфери для забезпечення їхньої інформаційної безпеки.

Користувачі інформаційних засобів організації повинні підписувати відповідні зобов'язання з конфіденційності (угода про нерозголошення). Зазвичай службовці підписують такі зобов'язання як частина основних умов приймання на роботу. Договір про дотримання конфіденційності інформації повинен переглядатися при зміні умов прийому на роботу або контрактних умов, особливо у тому випадку, коли службовець має намір звільнятися або при закінченні терміну дії контракту.

Інформаційні ресурси «ЯВІР ДНІПРО-1» діляться на три групи:

- Інформацію, яка є комерційною таємницею;
- Конфіденційна інформація;
- Строго конфіденційна інформація.

Після оцінки інформаційних активів підприємства необхідно провести їх ранжування для подальшого визначення актуальних та неактуальних загроз. Залежно від рангу, слід вживати технічні заходи для забезпечення захисту. Результати ранжування активів «ЯВІР ДНІПРО-1» представлені в таблиці 1.2.

Таблиця 1.2 - Результати ранжирування активів

Найменування активу	**Цінність активу (ранг)**
Відомості ділового характеру	4
Інформаційний актив з торговельно-економічних питань	4
Інформаційний актив про послуги, що надаються	5
Інформаційний актив з питань забезпечення безпеки	5
Інформаційний актив по організаційно-управлінської діяльності	2
Товар підприємства	3
Устаткування	3

Активи, які мають найбільшу цінність (детальніше розглянуті в табл. 1.3):

1. Інформаційні активи про зроблені послуги;
2. Інформаційні активи з питань забезпечення безпеки;
3. Відомості з чисто діловим характером;
4. Інформаційні активи з торговельно-економічних питань;
5. Товари організації;
6. Устаткування;
7. Інформаційні активи з організаційно-управлінської діяльності.

1.3.2 Оцінка вразливостей активів підприємства

Щороку загрози злому інформаційних систем і компрометації даних стають все більш і більш актуальними, більше того вектор загрози зміщується від простих методів до серйозних, продуманих і нетривіальних атак. За результатами третього кварталу 2023 року експерти Positive Technologies відзначили зростання кількості цілеспрямованих атак в порівнянні з 2022 роком рис. 1.2 [21].

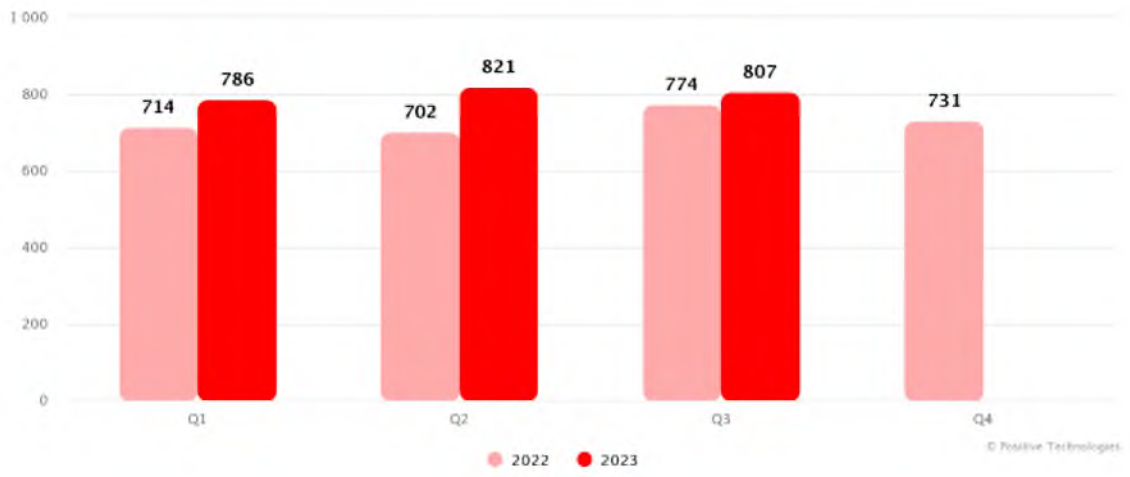


Рисунок 1.2 - Статистика росту цільових атак

Такі атаки відомі як APT-атаки (Advanced Persistent Threat), і вони спрямовані на конкретну організацію, галузь промисловості або бізнес. За даними 2023 року в успішних атаках на приватних осіб зловмисники застосовували різні канали соціальної інженерії. Найчастіше злочинці

використовували фішингові сайти (54%) та електронні листи (27%), а також вибудовували шахрайські схеми у соціальних мережах (19%) та месенджерах (16%) рис. 1.3.

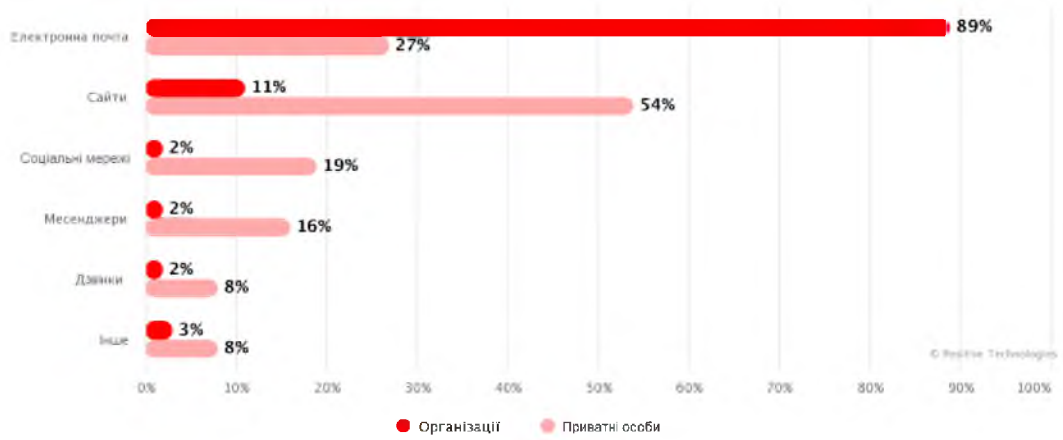


Рисунок 1.3 - Канали соціальної інженерії, які використовуються зловмисниками

Вищим керівництвом організації «ЯВІР ДНІПРО-1», в особі директора, було сформульовано чітке положення щодо інформаційної політики безпеки для всіх підрозділів організації. Політика безпеки виникла в результаті спільних зусиль технічного персоналу, що включає фахівця з кібербезпеки та системного адміністратора, які можуть розуміти всі аспекти політики та її реалізації, а також директора, який може впливати на проведення політики в життя.

У одному з положень цього документу вказано, що для забезпечення підтримки високого рівня інформаційної безпеки щорічно проводитиметься внутрішній аудит, який буде побудований в повній відповідності до правових і законодавчих норм з аудиторської діяльності в Україні. Під час аудиту буде використовуватися детальний аналіз ризиків, який включає оцінку вразливості активів.

Вразливість інформації визначається як можливість виникнення умов, при яких з'являється можливість реалізації загрози безпеки для даних.

Наявність вразливостей не завдає шкоди сама по собі, оскільки для цього потрібно наявність відповідних загроз. Проте, важливо фіксувати вразливості і регулярно перевіряти їх на випадки зміни ситуації.

Такі види оцінок передбачають ідентифікацію вразливостей в навколишньому середовищі, організаційних структурах, процедурах, персоналі, менеджменті, адміністрації, апаратних засобах, програмному забезпеченні або апаратурі зв'язку, які можуть бути використані джерелами загроз для завдання збитку активам та ефективному функціонуванню організації. Важливо відзначити, що некоректно використані та неправильно працюючі захисні заходи можуть стати джерелом виникнення вразливостей. Поняття «вразливості» може бути віднесене до властивостей або атрибутів активів, які використовуються іншим чином або для іншої мети, ніж та, для якої отримувалися або виготовлялися ці активи [17].

Початкові дані для оцінки вразливостей повинні надходити від власника або користувача активів, фахівця з обслуговуючих пристроїв, експерта з програмних і апаратних засобів систем інформаційних технологій.

Результати оцінки вразливостей активів «ЯВІР ДНІПРО-1» представлені в таблиці 1.3.

Під час аудиту будуть надані висновки у письмовій формі, з переліком усіх виявлених та оцінених вразливостей, для подальшого визначення сумарних ризиків. Це дозволить вибрати комплекс заходів щодо захисту даних.

1.3.3 Оцінка загроз активам

Метою оцінки можливостей порушників у реалізації загроз безпеки інформації є створення припущень щодо типів та видів порушників, які можуть втілювати загрози безпеки інформації в інформаційній системі з визначеними структурно-функціональними характеристиками та особливостями функціонування. Також важливо визначити потенціал цих порушників та можливі способи реалізації загроз безпеки інформації.

Таблиця 1.3 - Результати оцінки вразливості активів «ЯВІР ДНІПРО-1»

Зміст вразливостей	**Групи активів вразливості**						
	№1	**№2**	**№3**	**№4**	**№5**	**№6**	**№7**
1. Середовище і інфраструктури							
Неправильне застосування фізичних засобів управління доступу у будівлі	низький	низький	низький	низький	низький	низький	низький
Нестабільна робота електромережі	низький	низький	низький	низький	-	середній	низький
2. Апаратне забезпечення							
Відсутність схем періодичних замін	-	-	-	-	-	середній	-
Відсутність контроль за зміною конфігурацій	-	-	-	-	-	низький	-
3. Програмне забезпечення							
Відсутність механізму ідентифікації і автентифікації	низький	низький	низький	низький	-	-	низький
Відсутність аудиторських перевірок	низький	низький	низький	низький	низький	низький	низький
Неконтрольоване завантаження і застосування програмного забезпечення	низький	низький	низький	низький	-	середній	низький
4. Комунікація							
Незахищеність ліній зв'язку	висока	високий	високий	високий	-	високий	високий
Відсутність ідентифікації і автентифікації відправника і одержувача	високий	високий	високий	високий	-	високий	високий
Відсутність підтвердження посилок або отримань повідомлень	високий	середній	середній	середній	-	середній	середній
5. Документ (документообіг)							
Зберігання в незахищеному місці	низький	низький	низький	низький	-	-	низький
Безконтрольне копіювання	низький	низький	низький	низький	-	-	низький

З урахуванням наявності прав доступу та можливостей для отримання інформації та доступу до компонентів інформаційної системи, порушники поділяються на два основних типи:

1. зовнішні порушники (тип I) - особи, що не мають права доступу до інформаційної системи та її окремих компонентів. Вони реалізують загрози безпеки інформації ззовні інформаційної системи;

2. внутрішні порушники (тип II) - особи, що мають право постійний або разовий доступ до інформаційної системи та її окремих компонентів.

Оцінка загроз активам є наступним кроком після детального аналізу ризиків та оцінки вразливостей цих активів. Загрози будуть виявлені під час внутрішнього аудиту, який затверджений у письмовому положенні про інформаційну безпеку, в особі вищого керівника ланки організації «ЯВІР ДНІПРО-1» - директори, який покладає обов'язки з проведенню внутрішнього аудиту на системного адміністратора.

Загрози, або потенційні можливості несприятливих дій, володіють здатністю завдати шкоди системам інформаційних технологій та їх активам. Якщо ці загрози будуть реалізовані, вони можуть взаємодіяти з системами та призвести до небажаних інцидентів, які можуть негативно вплинути на систему. Загрози можуть мати різноманітне походження, включаючи природні та людські чинники, і їх реалізація може бути випадковою або умисною.

Класифікація можливості реалізації загрози (атаки) - це сукупність можливих варіантів дії джерел загрози за допомогою певних методів реалізації, використовуючи вразливості. Ці методи спрямовані на досягнення мети атаки. Важливо відзначити, що мета атаки може не завжди співпадати з цілями реалізації загрози і може бути націлена на отримання проміжних результатів, необхідних для досягнення загальної мети в майбутньому. У випадках, коли ці мети не співпадають, атаку може розглядатися як «підготовку до здійснення» протиправних дій. Результатами атаки є наслідки, які можуть виявитися реалізацією загроз або сприяти таким реалізаціям.

Існує достатньо велика кількість різнопланових загроз безпеці інформації різного генезису. Застосовується різноманітні види класифікацій, де в якості критеріїв ділення використовують види породженої небезпеки, ступінь злого наміру, джерела появи загрози і так далі. Далі опишемо найбільш просту систему класифікації загроз:

1. Природна загроза: Викликана дією об'єктивного фізичного процесу або стихійного, природного явища, незалежного від людини.

2. Штучна загроза: Викликана діяльністю людей. Серед штучних загроз, враховуючи мотивацій дій, можна виділити:

- ненавмисна (випадкова) загроза, викликана помилкою в проєктуванні захищеного елементу, помилкою в програмному забезпеченні, помилкою персоналу і т.д.;

- навмисна загроза, пов'язана із корисливим мотивом людини (зловмисників).

Загрози безпеки інформації можуть бути реалізовані порушниками через [18]:

1. несанкціонований доступ і (чи) вплив на об'єкти на апаратному рівні (програми (мікропрограми), вбудовані в апаратні компоненти (чіпсети));

2. несанкціонований доступ і (чи) вплив на об'єкти на загальносистемному рівні (базові системи введення-виводу, гіпервізори, операційні системи);

3. несанкціонований доступ і (чи) вплив на об'єкти на прикладному рівні (системи управління базами даних, браузери, веб-додатків, інші застосовні програми загального і спеціального призначення);

4. несанкціонований доступ і (чи) вплив на об'єкти на мережевому рівні (мережеве обладнання, мережеві застосування, сервіси);

5. несанкціонований фізичний доступ і (чи) вплив на лінії, (канали) зв'язки, технічні засоби, машинні носії інформації;

6. вплив на користувачів, адміністраторів безпеки, адміністраторів інформаційної системи або обслуговуючий персонал (соціальна інженерія).

Таблиця 1.4 - Результати оцінки загроз активам

Зміст вразливостей	**Групи активів вразливості**						
	№1	**№2**	**№3**	**№4**	**№5**	**№6**	**№7**
1. Загроза, обумовлена умисними діями							
Розкрадання	низький	низький	низький	низький	низький	низький	низький
Навмисне ушкодження	низький	низький	низький	низький	низький	низький	низький
Нелегальне проникнення зловмисників під виглядом санкціонованих користувачів	високий	високий	високий	високий	-	середній	середній
Імпорт/Несанкції експорт програмного забезпечення	низький	низький	низький	низький	-	низький	низький
Загроза зіткнення з шкідливим програмним забезпеченням	низький	низький	низький	низький	-	середній	низький
Перехоплення інформації	високий	високий	середній	середній	-	-	середній
Зміна сенсу переданої інформації	високий	середній	високий	середній	-	-	середній
2. Загроза, обумовлена випадковими діями							
Помилка при обслуговуванні	низький	низький	низький	низький	-	низький	низький
Апаратні відмови	низький	низький	низький	низький	низький	середній	низький
Помилки оператора	середній	середній	середній	середній	низький	середній	середній
Технічні несправності мережевих компонентів	низький	низький	низький	низький	-	низький	низький
Збоїв у функціонуванні послуг зв'язку	середній	низький	середній	середній	-	низький	середній
3. Загроза, обумовлена природними причинами (природний, техногенний чинник)							
Коливання напруги	низький	низький	низький	низький	-	низький	низький
Погіршення стану середовища, що запам'ятовує інформацію	-	-	-	-	-	низький	-

Під час перевірки буде складено письмовий звіт із докладним переліком всіх виявлених та оцінених загроз. Це необхідно для визначення сукупної оцінки ризиків, що буде використовуватися при виборі комплексу заходів з захисту інформації. Результати оцінки загроз активам «ЯВІР ДНІПРО-1» будуть представлені в таблиці 1.4.

1.3.4 Оцінка існуючих і планованих засобів захисту

Оскільки «ЯВІР ДНІПРО-1» є невеликим комерційним підприємством, як по кількості співробітників, так і за обсягом послуг, що надаються на ринку, положення про інформаційну безпеку було розроблено всередині організації під керівництвом директора.

У цьому письмовому положенні визначені завдання з забезпечення ІБ, які покладаються на спеціаліста з питань кібербезпеки та системного адміністратора. Перевірка передбачає проведення внутрішнього аудиту, результати якого узагальнюються у письмовій формі і передаються директору для остаточного рішення щодо впровадженню або вдосконалення захисних заходів [13].

Інформаційна система організації, яку ми розглядаємо, представляє собою сукупність робочих станцій і серверів, об'єднаних в єдину локальну мережу. Дані зберігаються і обробляються як на робочих станціях, так і на файловому сервері.

Локальна комп'ютерна мережа (ЛКМ) розглядають з урахуванням єдиних концептуальних положень, що є основою сучасних обчислювальних мереж в організаціях. Це положення передбачає використання загальних принципів побудови і однорідного активного мережевого обладнання. У структурі мережі компанії визначається ієрархія рівнів ЛКМ реалізується на базі стандарту Ethernet 10/100/1000 Base-T. Використання цього стандарту дозволяє ефективно забезпечити стабільне функціонування мережі. Конфігурацію мережі представлено в табл. 1.5.

Таблиця 1.5 - Конфігурація мережі підприємства

Компоненти характеристики	Реалізація мережі
Топологія	Зірка
Лінія зв'язку	Неекрановані виті пари категорії 5
Мережеві адаптери	Ethernet 10/100/1000 Base-T
Комунікаційне устаткування	Комутатори Ethernet 10/100/1000 Base-T
Спільне використання	Підключення мережевого принтера і МФУ через інтернет-мережу
Периферійних пристроїв	Комп'ютер до мережевого кабелю. Управління чергою до принтера здійснюють за допомогою програмного забезпечення комп'ютерів.
Підтримувані	Організація колективної роботи в середовищі
додатки	Електронного документообігу, робота з базами даних.

На підприємстві в серверній кімната №10 (Додаток В) встановлено джерело безперебійного живлення Eaton 9SX 6000i RT3U, та сервер ARTLINE Business T19 (T19v12).

Сервер використовується для резервного копіювання даних з ПК працівників або в разі необхідності, після чого ці дані зберігаються на сервері для подальшої обробки та роботи з ПЗ, які вимагають обмеженого доступу.

Це високотехнологічний маршрутизатор з підтримкою функції роутера Cisco RV325 (RV325-WB-K9-G5) дозволяє встановити значну кількість бездротових з'єднань у межах роботи локальної мережі з високим рівнем надійності.

У офісі для кожного співробітника встановлений окремий комп’ютер. Усі 10 комп’ютерів мають однакові характеристики: монітор MSI 23.8" IPS (1920x1080) Full HD та системний блок HP ProOne 440 G4 (4YV99ES) з характеристиками якого наведено в таблиці 1.6.

Таблиця 1.6 - Характеристики робочих місць

Назва	Характеристики	
ПК1-ПК10	Материнська плата	Intel B460
	Процессор	Intel Core i5-9700F (3.0 - 4.7 ГГц)
	ОЗУ 16 ГБ, DDR4-2933 МГц	8 ГБ DDR4-2666 МГц
	Відео карта	nVidia® GeForce® RTX 2060, 6144 МБ
	Блок живлення	550W
	Накопичувач	SSD 500
	Мережевий контроллер	Realtek RTL8111H

Конфігурацію периферійного обладнання наведемо у таблиці 1.7.

Таблиця 1.7 - Конфігурацію периферійного обладнання

Найменування	Кількість шт.
Принтеры Hewlett Packard LaserJet P2015 (A4. 1200dpi, 26 ppm, 32Mb, USB 2.0)	7
МФУ Canon LaserBase MF3110 (A4; 1200x600 dpi; 250 лист., 64mb)	1
Стационарный многофункциональный телефон Huarvei FT2050	25

Технічну архітектуру представимо на рис. 1.4.

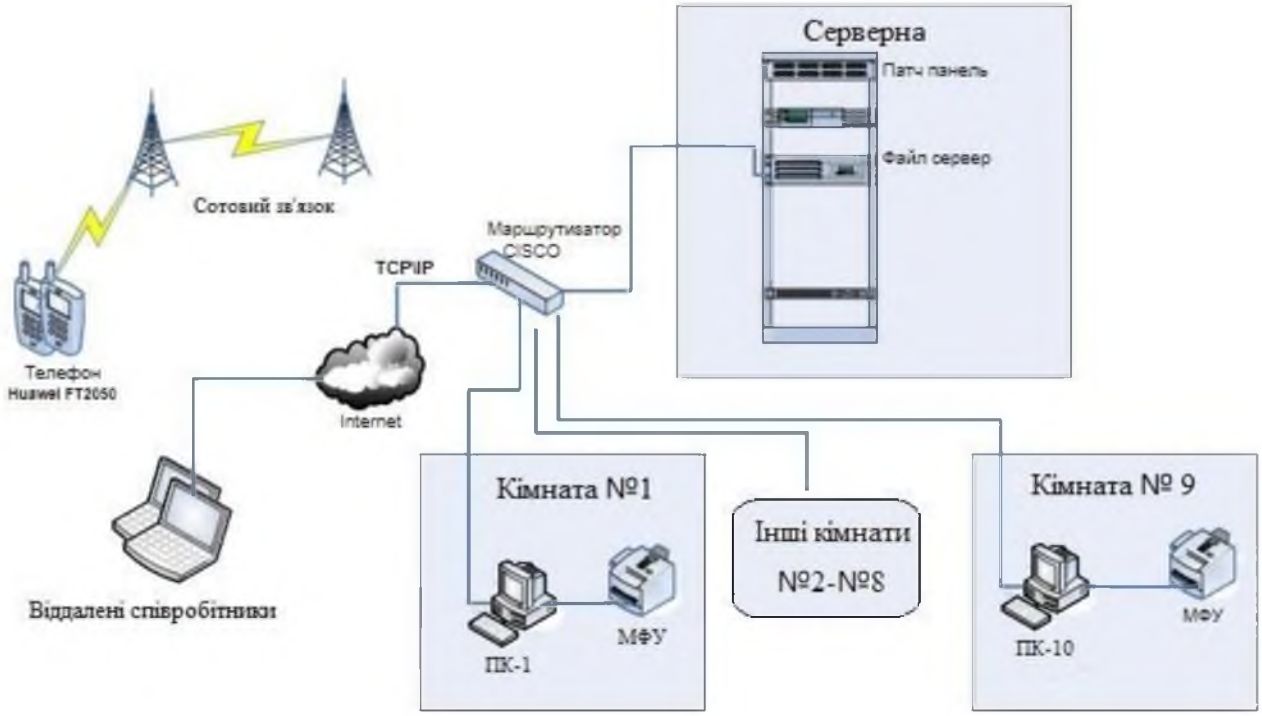


Рисунок 1.4 - Технічну архітектуру ІС «ЯВІР ДНІПРО-1»

Основне ПЗ, встановлене на підприємстві:

- ОС Windows Server 2019 Standard Edition, встановлено на сервері С1;

- ОС Microsoft Windows 10 Pro SP1 64-bit (визначаються функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та має експертний висновок №1027 дійсний з 26.09.2019) встановлено на всіх офісних ПК;

- Microsoft Office 2016 Pro, встановлено на всіх офісних ПК і сервері С1;

- CRM система для обліку клієнтів, встановлена сервері С1;

- Бухгалтерія BAS1C (тільки на комп'ютерах бухгалтерів та сервері);

- Бухгалтерія МЕДОК (тільки на комп'ютерах бухгалтерів та сервері);

- Антивірус NOD32 корпоративна версія на 15 ПК, ліцензія на 2 роки.

Програмна архітектура «ЯВІР ДНІПРО-1» представлена на рис. 1.5.

По периметру усієї території, приміщення «ЯВІР ДНІПРО-1» розташовані 7 камер відеоспостереження фірми Germikom (модель D - 250). Завдяки постійному відеоспостереженню фізичне розкрадання матеріальних об'єктів стає майже неможливим.

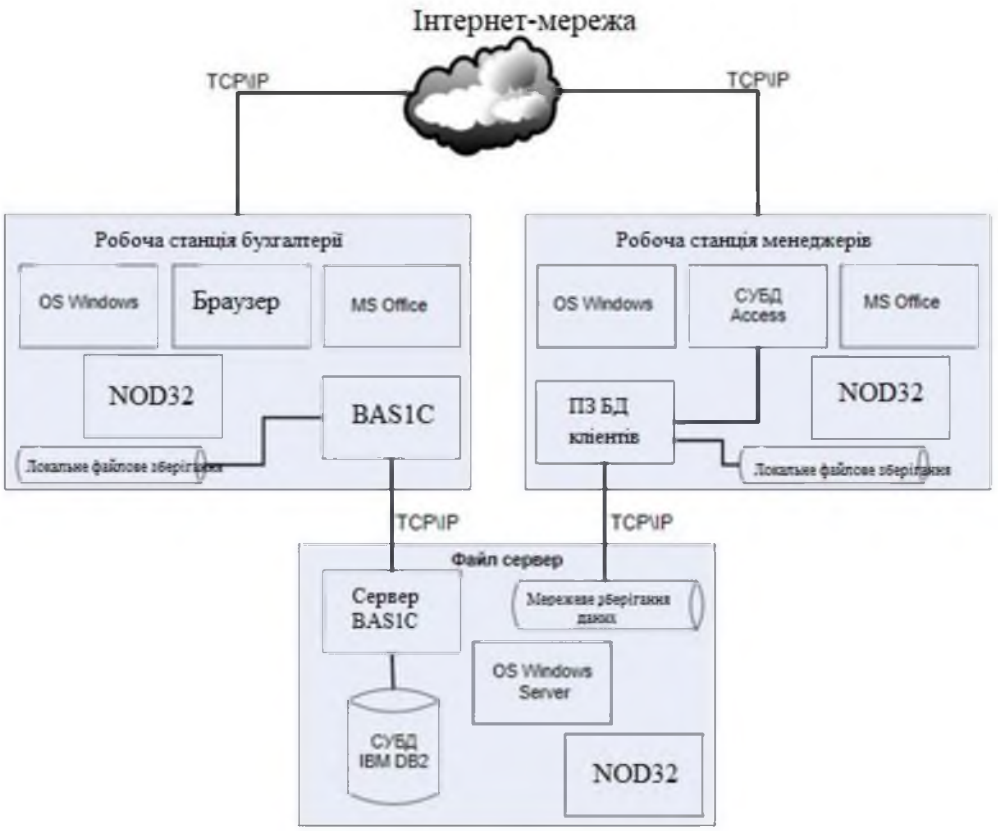
Аналіз виконання основних завдань по забезпеченню інформаційної безпеки «ЯВІР ДНІПРО-1» представлено в таблиці 1.8.

Таблиця 1.8 - Виконання основних завдань ІБ

Завдання по забезпеченню інформаційної безпеки даних	**Міра виконання**
Забезпечити безпеку виробничо-торгової діяльності, захист інформації і відомостей, що є комерційною таємницею	Не у повних об'ємах, наявність захисту тільки від фізичного доступу
Організувати роботу по правовому, організаційному і інженерно-технічному (фізичною, апаратною, програмною і математичною) захисту комерційних таємниць;	Не у повних об'ємах, виконана стандартними вбудованими засобами апаратури і програми.
Організувати спеціальне діловодство, яке виключає несанкціоноване отримання даних, що є комерційною таємницею;	У повних об'ємах
Запобігти необґрунтованому допуску і відкритому доступу до відомостей і робіт, що становлять комерційну таємницю;	Не у повних об'ємах, наявність захисту тільки від фізичного доступу
Виявити і локалізувати можливі канали витоку конфіденційних даних в процесах повсякденної виробничої діяльності і в екстремальних (аварії, пожежі та ін.) ситуаціях;	Не у повних об'ємах, виконується стандартними вбудованими засобами апаратури і програм.
Забезпечити режим безпеки при здійсненні таких видів роботи, як різні зустрічі, переговори, наради, засідання і інші заходи, які пов'язані з діловою співпрацею;	У повних об'ємах
Забезпечити охорону територій, будівель приміщень, з даними, що захищаються.	У повних об'ємах

Значить, з використанням програмних і апаратних засобів в «ЯВІР ДНІПРО-1» повинні вирішуватися наступні завдання:

1. Створення загальнодоступних баз даних;
2. Забезпечення спільної роботи користувачів фірми над інформацією;
3. Проведення централізованого резервного копіювання всієї інформації;
4. Здійснення контролю за доступом до даних;
5. Спільне застосування апаратних засобів і програмного забезпечення.



Малюнок 1.5 - Архітектура ІС «ЯВІР ДНІПРО-1»

1.3.5 Оцінка ризиків

У затвердженому положенні директора організації «ЯВІР ДНІПРО-1» з питань інформаційної безпеки встановлено, що під час перевірки внутрішнім аудитом, покладеним на посаду системного адміністратора, на завершальному етапі буде представлено укладення у письмовій формі звіту щодо сумарної оцінки ризику. Ця оцінка проводитиметься з використанням детального аналізу ризику для подальшого вибору комплексу заходів з захисту інформації.

Раніше всі дані про активи організації були зібрані від їхніх власників, оцінені, виявлені вразливості і загрози. На завершальних етапах аналізу ризиків проводяться сумарна оцінка. Оцінки ризиків є визначенням співвідношення потенційних негативних чинників на ділову діяльність у випадках небажаного інциденту, а також рівнів оціненої загрози і вразливих місць.

Ризики фактично представляють собою заходи незахищеності систем та пов'язаних з ними організацій. Величина ризиків залежить від наступних чинників:

- цінності активу;

- загроз і ймовірності виникнення подій, небезпечних для активу;

- легкості реалізації загрози в вразливому місці з вчиненням небажаних дій;

- наявності або планованого засобу захисту, що зменшує рівень вразливостей, загроз і небажаних дій [12].

Варто відзначити, що вибір методики оцінки ризику лежить повністю на розсуді особи, яка проводить цей аналіз. У нашому випадку це обов'язок системного адміністратора. Основним визначальним фактором у виборі є те, щоб обрана методика була зручною для самої організації і надавала довіру. У даному випадку вибрана методика, яка використовує матрицю у вигляді таблиці з заздалегідь визначеними значеннями.

Сама оцінка відбувається наступним чином: ідентифікують відповідні рядки матриці за цінністю активів і відповідні стовпці за мірою загроз і вразливостей. Наприклад, якщо цінність активу дорівнює 4, загроза характеризується як «висока», а вразливість - як «низька», то міра ризику дорівнює 5.

Якщо існує вразливе місце без відповідних загроз або загроза без відповідних вразливих місць, то вважаються, що наразі ризики відсутні.

Показник ризику у використовуваній таблиці вимірюється в шкалах від 0 до 8 із такими визначеннями рівня ризиків:

1 - ризики практично відсутні; теоретично можлива ситуація, при якій подія може настати, але на практиці це відбувається рідко, і потенційний збиток порівняно невеликий;

2 - ризики дуже малі; подія подібного роду трапляється досить рідко, крім того, негативні наслідки невеликі;

8 - ризики дуже великі; події ймовірно настануть, і наслідки будуть дуже серйозні і т. д..

Використовувана для оцінки шкала представлена в таблиці 1.9.

Таблиця 1.9 - Оцінки ризиків

	Рівні загрози	Низька			Середня			Висока		
	Рівні вразливості	Н	С	В	Н	С	В	Н	С	В
Цінність активів	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Результат проведення оцінок ризиків «ЯВІР ДНІПРО-1» представимо в таблиці 1.10.

Таблиця 1.10 - Результати оцінки ризиків «ЯВІР ДНІПРО-1»

Ризик (у штрафних балах)	Актив	Ранг ризику
61	Інформаційний актив про послуги, що надаються	1
60	Інформаційний актив з питань забезпечення безпеки	2
47	Відомості ділового характеру	3
46	Інформаційний актив по торгово-економічним питанням	4
27	Устаткування	5
22	Інформаційний актив по організаційно-управлінської діяльності	6
6	Товар організації	7

1.4 Характеристика комплексу завдань, завдання і обґрунтування необхідності розробки структури VPN мережі підприємства

1.4.1 Вибір комплексу завдань

Виходячи з проведеного аналізу ризиків у пункті 1.3.5, в організації «ЯВІР ДНІПРО-1» існують наступні види загроз безпеки інформації, для яких буде розроблена система захисту:

- Загрози порушення конфіденційності даних;
- Загрози порушення цілісності даних;
- Загрози порушення доступності;
- Загрози порушення спостереження даних;
- Загрози порушення автентичності інформації.

Для кожної з вищезазначених загроз буде визначено відповідні послуги захищених систем, а саме: послуги конфіденційності, цілісності, доступності, спостереження і автентичності. Системи при цьому вважаються захищеними або безпечними, якщо забезпечуються всі вище перелічені послуги.

1.4.2 Визначення місця проєктованого комплексу завдань

Виходячи з раніше проведеного аналізу ризиків і враховуючи актуальні загрози і вразливості, місцем, де будуть розроблятися комплексні організаційні і інженерно-технічні заходи з забезпечення інформаційної безпеки, визначена локальна обчислювальна мережа компанії «ЯВІР ДНІПРО-1».

Одним із основних завдань для нормального функціонування ЛКМ і для успішного проведення бізнес-процесів є забезпечення безпеки інформаційних потоків, що циркулюють в ній. На даному етапі існуючі засоби інформаційної безпеки в організації обмежені вбудованими засобами використовуваного ПЗ, наприклад, захисними механізмами операційної системи, що наразі не забезпечують надійного захисту.

Для ЛКМ будуть в обрані такі засоби забезпечення захисту, які мінімізують шанс виникнення загроз, вразливостей і ризиків. Іншими словами,

мережа, яка на даний момент існує в компанії, буде забезпечена високим рівнем захисту.

1.5 Вибір захисних заходів інтернет-мереж

1.5.1 Вибір організаційних заходів

Організація повинна визначити свою стратегію захисту інформації, обираючи між оборонною, наступальною та попереджувальною стратегіями. Стратегія визначає загальну спрямованість діяльності організації з урахуванням об'єктивних потреб, можливих умов здійснення цієї діяльності та можливостей самої організації.

Після проаналізування характеристик усіх трьох стратегій та змісту етапів побудови засобів захисту інформації, в «ЯВІР ДНІПРО-1» було прийнято рішення на користь наступальної стратегії захисту інформації [22]:

- Забезпечуваний рівень захисту: Може бути дуже високим, але лише в межах існуючих уявлень про природу загроз інформації та можливості їх прояву.

- Умови, необхідні для реалізації:

1. Наявність переліку та характеристик повної великої кількості потенційно можливих загроз інформації;

2. Можливість використати різні методи і засоби захисту;

3. Наявність можливостей впливу на архітектуру ЛКМ і технологію обробки інформації.

- Ресурсоємність: Значна, із зростанням вимог до захисту, ресурси збільшуються експоненційно.

- Рекомендації по застосуванню: При порушенні захищеності інформації виникає загроза значних фінансових і інших втрат.

На вибір вплинув наступний зміст етапів побудови засобів захисту:

1. Формування середовища захисту;

1.1. структурована архітектура ЛКМ;

1.2. структурована технологія обробки інформації, яку захищають, і чітка організація обробки захищеної інформації.

2. Аналіз засобів захисту;

2.1. Представлення організаційно-структурної побудови ЛКМ у вигляді впорядкованого графа: вузли - типові структурні компоненти, дуги - взаємозв'язки між компонентами;

2.2. Представлення технології обробки інформації, яку захищають, у вигляді строго певної схеми;

2.3. Визначення параметрів інформації, яку захищають, та умов її обробки.

3. Оцінки вразливості інформації;

3.1. Визначення значень вірогідності порушення інформації, яку захищають, в умовах, в яких вона оброблятиметься;

3.2. Оцінка розміру можливого збитку при порушеннях захищеності інформації.

4. Визначення вимог до захисту;

Визначення вірогідності надійного захисту інформації, яка має бути забезпечена при обробці інформації, що захищається.

5. Побудова системи захисту;

Вибір типового варіанту або проєктування індивідуальної системи захисту.

6. Організація функціонування систем захисту;

Розробка технології функціонування системи захисту.

7. Вимоги до середовища захисту;

Визначається залежно від вимог до захисту інформації.

Організаційні заходи відіграють ключову роль у реалізації надійних механізмів захисту даних. Можливість несанкціонованого використання конфіденційної інформації в значній мірі зумовлені як технічним аспектом, так і злочинними діями, або недбалістю користувача.

Організаційні заходи забезпечення захисту ґрунтуються на законодавчих і нормативних документах з питань безпеки даних. Вони мають охоплювати всі ключові аспекти збереження ресурсів. Для досягнення цієї мети слід вжити такі заходи:

- обмежити фізичний доступ до об'єктів ІС та впроваджувати режимні заходи;

- зменшити можливість перехоплення даних через наявність фізичних полів;

- обмежити доступ до інформаційних ресурсів та інших елементів ІС, встановивши правила розмежування доступів, а також криптографічне закриття каналу передачі даних;

- створити резервні копії важливої інформації для запобігання втратам у разі аварій;

- здійснювати профілактичні заходи для запобігання впровадженню вірусів та інших загроз.

До обов'язкових організаційно-правових заходів захисту, необхідних для організації в «ЯВІР ДНІПРО-1» відносяться:

- організація і підтримка надійного пропуску та контроль відвідувачів фірми;

- забезпечення надійної охорони приміщень компанії та її території;

- організація захисту інформації, включаючи призначення відповідальної особи за захист інформації, систематичний контроль за роботою персоналу та порядком обліку, зберігання і знищення документів.

Організаційні заходи щодо роботи з персоналом компанії передбачають:

- проведення співбесіди під час прийому на роботу;

- ознайомлення з правилами та процедурами роботи з інформаційними системами в організації;

- надання інструкцій з правильної експлуатації інформаційних систем для забезпечення їхньої цілісності та коректності.

Для забезпечення адміністративного рівня в організації був набраний наступного вигляду документів:

1) Керівництво для користувача;

Документація на програмні та апаратні засоби, що містить коротке керівництво для користувача з описом основних функцій.

2) Керівництво по комплексним засобам захисту;

Цей документ призначений для системного адміністратора, відповідальному за захист і повинен містити:

- опис контрольованих функцій;

- керівництво по впровадженню засобів захисту;

- описи процедур старту програмних і апаратних засобів, процедури перевірки правильності старту та роботу з засобами реєстрації.

3) Загальна політика безпеки;

У документі визначені цілі, сфера застосування та сама політика, яку прийнято в організації «ЯВІР ДНІПРО-1».

4) Тестова документація;

Цей документ містить опис тестів і випробувань, яким були піддані засоби обчислювальної техніки, а також результати тестування.

1.5.2 Вибір інженерно-технічних заходів

Побудова системи захисту інформації з точки зору способу реалізації проводитиметься шляхом модернізації існуючої системи. Робота по інженерно-технічному захисту інформації на підприємствах включає два етапи: модернізацію системи захисту та підтримку захисту на необхідному рівні.

Модернізація системи захисту інформації та підтримка її на необхідному рівні передбачає проведення наступних основних робіт:

- уточнення переліку джерел інформації та носіїв інформації, що захищаються, виявлення та оцінка загроз безпеки інформації;

- визначення заходів по захисту інформації, викликаних зміною цілей і завдань захисту, а також загроз безпеки інформації;

- контроль ефективності заходів.

Перед вибором конкретних програмно-технічних засобів проведемо аналіз основних технологій, які застосовуються в сучасний час для забезпечення захищеної ЛКМ [19]:

1. Virtual Personal Network (VPN) рішення;

Поширення глобальної мережі передачі даних відкриває великі можливості для об'єднання територіально розкиданих локальних мереж організацій та створення приватних віртуальних мереж (VPN). У цьому випадку глобальні мережі виконують роль транспортного компонента, який об'єднує локальні мережі в єдину інформаційно-обчислювальну систему. VPN створювалися і до стрімкого росту глобальних мереж, але для їх об'єднання використовувалися виділені канали передачі даних, що призводило до таких проблем, як висока вартість оренди каналів та жорстка прихильність до місця розташування.

Наприклад, при переїзді офісу компанії, яка має розгорнутий сегмент локальної мережі, пов'язаний виділеним каналом із загальною мережею підприємства, виникали додаткові труднощі з подальшим підключенням локальної та загальної мереж.

З використанням комутованих каналів глобальних мереж передачі даних можна досягти гнучкості, масштабованості і універсальності при створенні VPN. Також розширення Інтернет дало можливість багатьом компаніям переводити частину персоналу на дистанційний режим роботи. У таких випадках співробітники зберігають постійний зв'язок з фірмою, наприклад, за допомогою системи електронного документообігу, при цьому проблема зв'язку з мережею офісу вирішуються провайдерами.

Потреба в забезпеченні безпеки мереж на основі протоколу IP постійно зростає. У сучасному бізнес-середовищі, де компанії сильно пов'язані за допомогою Інтернету, інтернет-мереж, дочірніх відділень і видаленого доступу, критична інформація постійно пересувається через мережеві кордони. Однією з ключових задач мережевих адміністраторів і фахівців інформаційної безпеки є забезпечення того, щоб цей трафік не підлягав:

- модифікації даних під час їх передачі по каналах;
- перехопленню, перегляду або копіюванню;
- доступу до даних з боку неавторизованих користувачів.

Ці проблеми часто позначають як забезпечення цілісності даних, конфіденційності і аутентифікації. Крім того, необхідно захищати інформацію від відтворення.

При вирішенні проблем передачі інформації через відкриті канали Інтернету широко використовуються рішення на основі VPN. VPN - це об'єднання декількох локальних мереж, які підключені до мережі загального призначення, в єдину віртуальну (логічно виділену) мережу. Засоби VPN формують захищений тунель між двома точками за допомогою криптографії. Крім того, вони надають широкі можливості для вибору алгоритмів аутентифікації, шифрування і перевірки цілісності потоку даних.

Використання VPN дозволяє легко консолідувати та оптимізувати ресурси компанії. Оскільки VPN працює через мережу Інтернет, компанія уникає значних витрат, пов'язаних із придбанням додаткового обладнання та орендою ліній зв'язку. Використання виділених (орендованих) ліній зв'язку може призвести до збільшення витрат до сотень тисяч доларів, що часто важко виправдати.

Головне достоїнство VPN - це можливість забезпечення безпеки багатьох комунікаційних потоків за допомогою одного механізму. VPN захищає веб-сайти, електронну пошту, файли через протоколи FTP, інтернет-відеоконференції та будь-які інші потоки даних, які використовують протокол TCP/IP. Конкретно, інформаційні потоки захищаються від небажаних одержувачів з використанням криптографічних методів.

VPN дозволяє уникнути багатьох загроз, зберігаючи цілісність і конфіденційність даних через шифрування та аутентифікацію за допомогою спеціальних протоколів і схем. Засоби VPN також захищають інформацію, пов'язану з транспортом IP-пакетів, від різних мережевих атак, таких як IP-spoofing і hijacking, а також вони захищені від атак типу man-in-the-middle.

Під час розробки ПЗ для створення VPN або його апаратної реалізації можуть виникнути вразливості. Однак, як правило, на практиці використовуються перевірені часом розробки, які регулярно оновлюються і виправляються.

Основні вимоги, які повинні виконувати рішення VPN, наступні:

- аутентифікація користувача. Засіб повинен надійно аутентифікувати віддаленого користувача VPN та допускати тільки авторизованих користувачів. Додатково, важливо забезпечити політику аудиту для відстеження активності користувачів: хто, коли і на який термін був підключений;

- управління IP-адресами. VPN-рішення повинно виділяти IP-адреси з відповідної підмережі та гарантувати їхню конфіденційність;

- шифрування даних. Всі дані, які передаються через публічні мережі, повинні бути зашифровані для забезпечення їхньої конфіденційності та непридатності для читання;

- управління ключовою інформацією. VPN-засіб повинен генерувати та регулярно оновлювати ключі для шифрування. Це забезпечить високий рівень безпеки та унеможливить розкриття ключової інформації.

2. Технологія екранування мережі;

Основні засоби захисту ЛКМ - це міжмережеві екрани. У літературі зустрічаються їх синоніми, такі як брандмауер, firewall, маршрутизатор, що фільтрує і ін. Під усіма цими термінами мається на увазі одне й те саме - одне функціональне призначення, але вони можуть містити різний набір інструментів захисту. Мережеві екрани - це лише інструментами системи безпеки. Мережевий екран - це засіб реалізації політики безпеки на мережевому рівні, який надає певний рівень захисту. Рівень безпеки, що надається мережевим екраном, може варіюватися залежно від вимог безпеки. Досягається традиційний компроміс між безпекою, простотою використання, вартістю, складністю і так далі. Мережевий екран – це лише один із механізмів, які використовують для управління і спостереження за доступом до мережі з метою її захисту.

Системою firewall замінюється маршрутизатор або зовнішній шлюз мережі. Захищену частину мережі розміщують за ним. Пакети, адресовані firewall, обробляються локально, а не просто переадресовуються. Пакети ж, які адресовані об'єктам, розташованим за firewall, не доставляються. З цієї причини хакерові доводиться мати справу із системою захисту firewall.

3. Системи Intrusion Detection System (IDS);

Системи визначення атак IDS моніторять інформаційну систему на мережевому і прикладному рівнях для виявлення порушень безпеки та оперативної реакції на них. Мережеві IDS є джерелами даних для аналізу мережевих пакетів.

Були запропоновано різні підходи до вирішення завдань виявлення атак. У загальному випадку розглядається умисна активність, яка включає, окрім атак, дії, виконані в рамках наданих повноважень, але політики безпеки, що порушують встановлені правила. Проте всі існуючі IDS розділяються на два основні класи: одні застосовують статистичний аналіз, інші - сигнатурний аналіз.

Існують два основних підходи до виявлення мережевих атак: аналіз мережевого трафіку і аналіз контенту. У першому випадку досліджуються лише заголовки мережевих пакетів, в другому - їх вміст. Однак повний контроль інформаційних взаємодій відбувається тільки за допомогою аналізу вмісту усіх мережевих пакетів, включаючи заголовки та області даних. Проте з практичної точки зору таке завдання важко виконати через великий обсяг даних, які доводиться обробляти. У сучасних IDS починаються серйозні проблеми з продуктивністю вже при швидкості 100 Мб/с в мережах. Тому для виявлення атак часто використовують аналіз мережевого трафіку, а в окремих випадках поєднують його з аналізом контенту.

Як вже зазначалося вище, відповідні продукти поділяються на системи IDS на базі мережі та на базі хоста. Обидві системи намагаються виявити вторгнення, але обробляють абсолютно різні дані. Система IDS на базі мережі для розпізнавання атак читає потік даних, схожий на аналізатор. Головним чином, вона складається з сенсорів, що реєструють усі мережеві пакети, інтерфейс яких підключений до призначеного для аналізу або копіювання порту комутатора. Концентратори можуть також застосовуватися для підключення такої системи до мережі.

Системи IDS на базі хоста використовують агенти, які функціонують як невеликі додаткові програми на контрольованих серверах або робочих місцях.

Вони аналізують активність на підставі журналів реєстрації та аудиту для пошуку ознак небезпечних подій.

Важливою ознакою якісних систем виявлення атак є не тільки, і не стільки, кількість трафіку, яку вони здатні контролювати та проаналізувати, але передусім, точність виявлення та наявність інструментарію у адміністраторів для додаткових стежень і аналізу вручну. В цьому випадку просто і швидше отримати інформацію про іншу протокольовану діяльність за тією ж самою початковою або кінцевою адресою - це тільки самий початок роботи.

3. Криптографія.

Криптографія використовується для вирішення трьох основних завдань:

- забезпечення конфіденційності даних;

- контроль цілісності даних;

- забезпечення достовірності авторства даних.

Для шифрування застосовується відкритий ключ, для розшифрування - закритий ключ. Відкритий ключ поширюється вільно.

Цифровий підпис захищає дані таким чином:

- для підписання даних використовується хеш-функція, за допомогою якої визначається хеш-сума початкових даних. По хеш-сумі можна визначити, чи мають місце які-небудь зміни в цих даних.

- отримана хеш-сума підписується цифровим підписом, дозволяючи підтвердити особу того, що підписало.

1.6 Висновок

Виходячи з аналізу ризиків в «ЯВІР ДНІПРО-1» існують наступні види загроз безпеки інформації, для яких розроблятиметься система захисту:

- Загрози порушення конфіденційності даних;

- Загрози порушення цілісності даних;

- Загрози порушення доступності;

- Загрози порушення спостереження даних;

- Загрози порушення автентичності інформації.

При розгляді загроз безпеки інформації в інтернет-мережах, можна помітити, що велика частина актуальних загроз в тому або іншому вигляді є ознаками APT -атаки.

Такими ознаками є:

1. Реалізація загрози підвищення привілеїв;

2. Реалізація загрози підміни програмного забезпечення;

3. Реалізація загрози несанкціонованого створення обліковому запису користувача;

4. Реалізація загрози впровадження коду або даних. Отже, матиме сенс впровадження засобу, здатного своєчасно виявити реалізацію певних загроз;

Рішення передбачається здійснити на базі комплексу програмних і програмно-апаратних засобів захисту інформації ТОВ «ТЕЛЕМАРТ» ViPNet Office Firewall. Це пакет програмного забезпечення включає в себе такі технології ViPNet: ViPNet Manager, ViPNet Coordinator, ViPNet Client і ViPNet IDS.

1. ViPNet Manager: Достатньо встановити його в одному з офісів компанії;

2. ViPNet Coordinator: Встановлюються на всіх ПК компанії, на вході в локальну мережу, а також на сервери-маршрутизатори. Він виконує роль міжмережевих екранів і криптошлюзів для організації захищених тунелів між видаленими локальними мережами;

3. ViPNet Client: Може бути встановлено як усередині локальних мереж на робочих станціях співробітників, так і на мобільних комп'ютерах для організації захищеного видаленого доступу до ресурсів локальних мереж. ViPNet Client в цьому випадку виконує роль персонального мережевого екрану і шифратора IP-трафіку;

4. ViPNet IDS: Використовує метод сигнатурного аналізу на основі набору правил для виявлення атак (вторгнень). Правила завантажуються в ViPNet IDS і регулярно оновлюються.

Під час роботи в захищеній мережі ViPNet Coordinator і ViPNet Client можуть фільтрувати звичайний, незашифрований IP-трафік, що дозволяє

забезпечити безперебійну роботу серверів та робочих станцій з відкритим доступом до ресурсів Інтернету або локальних мереж (таких як мережеві принтери, незахищені робочі станції і сервери).

ViPNet Office Firewall обладнаний повним набором необхідних сертифікатів, що робить його застосування для захисту даних абсолютно легітимним з точки зору українського законодавства.

Переваги:

- централізоване управління;
- висока пропускна спроможність;
- висока надійність і відмовостійкість;
- простота впровадження і експлуатації, що не вимагає розширення штату;
- можливість віддаленого оновлення ПЗ.

Можливості:

- криптографічний захист даних;
- міжмережеве екранування;
- забезпечення видаленого доступу;
- інтеграція з системами виявлення атак;
- проста масштабованість рішень;
- авторизоване навчання роботі з комплексом;
- сповіщення адміністратора (у режимі реального часу) про події, що вимагають оперативного втручання;
- абсолютна прозорість для всіх застосувань.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Комплекси організаційних заходів забезпечення інформаційної безпеки та захисту інформації підприємства

2.1.1 Нормативно-правові основи створення систем забезпечення інформаційної безпеки та захисту інформації в інтернет-мережах підприємства

Основою для формування організаційної системи забезпечення інформаційної безпеки та захисту інформації підприємства «ЯВІР ДНІПРО-1» є законодавча база, яка визначає 4 рівні правового забезпечення інформаційної безпеки підприємства.

Перший рівень правового захисту.

Для правового забезпечення інформаційної безпеки використовуються ряд законів та постанов щодо забезпечення інформаційної безпеки:

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

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.

- Закон України «Про державну таємницю» від 21.01.1994 № 3855 - XII

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

На другому рівні правової охорони інформації та захисту включаються ухвали Кабінету міністрів України (КМУ):

- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373.

- Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736.

Третій рівень правового забезпечення системи захисту економічних даних.

На даному рівні забезпечення правового захисту включає державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

- НД ТЗІ 3.7-003-2023: Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.

- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.

- НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі.

- НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

- НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

- НД ТЗІ 2.5-008-02: Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

- НД ТЗІ 2.5-010-03: Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу.

- НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

- НД ТЗІ 3.6-001-2000: Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

- Автоматизовані системи. Вимоги до змісту документів РД 50-34.698.

- Технічне завдання на створення автоматизованої системи. ГОСТ 34.602-89.

- НД ТЗІ 1.1-002-99: Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Також, до третього рівня безпеки інформаційних технологій відносяться керівні документи, норми, методи інформаційної безпеки і класифікатори, розроблені державними органами.

Четвертий рівень стандарту інформаційної безпеки.

До четвертого рівня стандарту інформаційної безпеки входять локальні нормативні акти, інструкції, положення та методи інформаційної безпеки, а також документація з комплексного правового захисту.

Європейські стандарти безпеки.

ISO 15408:2022 Common Criteria for Information Technology Security Evaluation висвітлює критерії для оцінки механізмів безпеки програмно-технічного рівня в міжнародному стандарті ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій), прийнятому в 1999.

Загальні критерії оцінки безпеки інформаційних технологій (далі "Загальні критерії") визначаються функціональними вимогами безпеки (security functional requirements) і вимогами до адекватності реалізації функцій безпеки (security assurance requirements).

ISO 27002:2022 Code of Practice for Infonnation Security Management.

Більш повно критерії оцінювання механізмів безпеки організаційного рівня представлені в міжнародному стандарті ISO 27002 Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою), прийнятому в 2000 році. ISO 27002 - це ніщо інше, як міжнародна версія британського стандарту BS 7799.

У ISO 27002 містяться практичні правила з управління інформаційною безпекою і можуть використовуватися як критерії при оцінці механізмів безпеки організаційного рівня, охоплюючи адміністративні, процедурні і фізичні заходи захисту.

Практичні правила визначаються 10 розділами:

1. Політика безпеки;

2. Організацію захисту;

3. Класифікацію ресурсів і їх контроль;

4. Безпека співробітників;

5. Фізична безпеку;

6. Адміністрування комп'ютерної системи і обчислювальної мережі;

7. Управління доступом користувачів;

8. Розробка і супровід інформаційної системи;

9. Планування безперебійних робіт в організаціях;

10. Контроль виконання вимог політик безпеки.

Ці розділи містять опис механізмів безпеки організаційного рівня, які вже застосовуються в урядових і комерційних організаціях багатьох країн світу. Десять засобів контролю, що пропонуються в ISO 27002 (їх відзначили як ключові), вважаються особливо важливими. Засоби контролю у даному контексті - це механізми управління інформаційною безпекою організації.

Такі засоби контролю є ключовими:

- Документ про політику інформаційної безпеки;

- Розподіл обов'язків для забезпечення безпеки;

- Навчання і підготовка персоналу для підтримки режимів інформаційної безпеки;

- Повідомлення про кожен випадок порушення захисту даних;

- Застосовування засобів захисту від вірусів;

- Планування неперебійної роботи організації;

- Контроль копіювання програмного забезпечення, яке захищається законами про авторське право;

- Захист документації організації;

- Захист даних;

- Контроль відповідності політикам безпеки.

У процедурі аудиту безпеки АС включені перевірка наявності вищезазначених ключових засобів контролю, оцінка повноти і правильності їх реалізації, а також аналіз їх адекватності ризикам, які існують в цьому

середовищі функціонування. Складовою частиною робіт з аудиту безпеки АС є також аналіз і управління ризиками.

Проєктована система повинна вирішувати наступні завдання:

- виявлення, попередження і ліквідація наслідків комп'ютерних атак, які спрямовані на контрольовані організацією інформаційні ресурси;

- проведення заходів за оцінкою міри захищеності ресурсів організації;

- проведення заходів по встановленню причин комп'ютерних інцидентів, викликаних комп'ютерними атаками;

- збір і аналіз даних про стан інформаційної безпеки в контрольованих організацією ресурсів;

- інформування зацікавлених осіб і суб'єктів загальної системи з питань виявлення, попередження і ліквідації наслідків комп'ютерних атак та інших подій.

2.1.2 Розробка алгоритму аналізу і обробки інцидентів комп'ютерної безпеки

Кістяк будь-якої системи моніторингу і управління подіями інформаційної безпеки - це агрегатор інформації і її аналізатор. Агрегатор збирає інформацію з різних джерел і упаковує її в необхідний для аналізатора формат. Аналізатор за зібраними даними формує повідомлення про інциденти інформаційної безпеки і оповіщає адміністратора інформаційної безпеки про наявність несанкціонованих дій в системі.

Щодня через інформаційні ресурси компанії проходить велика кількість інформації, електронної документації і авторизується декілька сотень тисяч клієнтів організації, що викликають більше п'ятисот тисяч всіляких подій, що помічаються системою виявлення вторгнення, антивірусами, міжмережевими екранами і т.д., з яких треба виділити інциденти, здійснені зловмисниками і спричиняючи за собою шкоду інформаційним ресурсам організації.

Фільтрація таких подій відбуватиметься шляхом порівняння подій з базою інцидентів і сигнатур, що вже має. Під базою інцидентів і сигнатур розумітимемо

- базу, що містить сукупність сигнатур заздалегідь внесених або отриманих від спеціаліста з питань кібербезпеки. Шляхом порівняння, апаратура зможе виділити з декількох тисяч подій пару сотень інцидентів, які надалі будуть детально проаналізовані системним адміністратором і вибрані ті з них, які можуть завдати шкоди інформаційним ресурсам підприємства. Після запобігання загрозі ресурсам, інциденти групуються і створюються картки інцидентів, які вносяться у базу інцидентів і сигнатур для навчання системи. Воронка інцидентів представлена на рис. 2.1.

Рисунок 2.1 - Воронка інцидентів

При виявленні інцидентів, що спричиняють інформаційну шкоду для підприємства, негайно інформується служба ІТ. Підтвердивши цей інцидент, відділ негайно реагує і приймає заходи для переривання інциденту та ліквідації його наслідків.

Отримуємо алгоритм роботи системи при обробці подій:

1. Моніторинг мережі, яку контролює організація;
2. Виявлення подій;
3. Апаратна фільтрація подій;
4. Повторний детальний аналіз інциденту обслуговуючим персоналом;
5. При підтвердженні інциденту - негайне реагування і контроль інциденту;
6. Внесення інциденту у базу інцидентів і сигнатур, усунення наслідків.

Цей алгоритм проілюстрований на рис. 2.2.

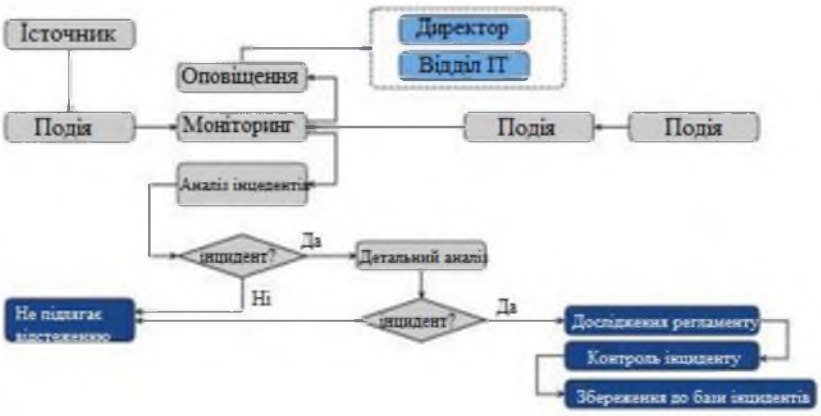


Рисунок 2.2 - Алгоритм аналізу і обробки інцидентів

2.1.3. Програмно-апаратні засоби для системи виявлення, попередження і ліквідації наслідків комп'ютерних атак

Атаки з підвищеним рівнем виникають, коли зловмисники використовують неправильну конфігурацію, помилки, слабкі паролі і інші уразливості, що дозволяють отримати доступ до захищених ресурсів. Типова атака розпочинається з отримання зловмисником доступу до облікового запису з низьким рівнем привілеїв. Після входу до системи зловмисники вивчають її з метою виявлення інших вразливостей, які вони можуть використати надалі. Потім вони використовують отримані привілеї для того, щоб видати себе за реальних користувачів, отримати доступ до цільових ресурсів і виконати різні завдання непоміченими.

Атаки з підвищенням рівня бувають вертикальними і горизонтальними. При вертикальному типі зловмисник дістається доступу до облікового запису і потім виконує завдання від імені цього користувача. При горизонтальному типі зловмисник спочатку отримує доступ до одного або декількох облікових записів з обмеженими привілеями, а потім компрометує систему для отримання додаткових прав на виконання адміністративних функцій.

Такі права дозволяють зловмисникам виконувати адміністративні завдання, впроваджувати шкідливе ПЗ або здійснювати інші небажані дії. Наприклад, вони можуть порушити роботу системи, змінити налаштування

безпеки, викрасти дані або скомпрометувати систему таким чином, що в ній залишаться відкриті «чорні ходи», які можна буде використати в майбутньому.

Виходячи з теми дипломної роботи, метою є підвищення рівня захищеності інтернет-мережі. Для досягнення цієї мети передбачено розробку системи виявлення, попередження і ліквідації наслідків комп'ютерних атак для «ЯВІР ДНІПРО-1». Ця система буде виконувати моніторинг мережі з метою виявлення подій, фільтрацію за заданими сигнатурами та подіями, а також виявлення інцидентів, які можуть завдати шкоди інформації і інформаційним ресурсам організації.

Для працездатності приведеного вище алгоритму нам необхідно:

1. Програмно-апаратний комплекс для моніторингу мережі і пошуку подій з дубльованого через SPAN порт, від маршрутизатора, трафіку мережі;

2. Програмно-апаратний комплекс для фільтрації подій;

3. Програмно-апаратний комплекс для адміністрування.

4. Постачальника сигнатур для програмно-апаратного комплексу події, що фільтрує.

Відповідно до закону України "Про електронні довірчі послуги" (Відомості Верховної Ради (ВВР), 2017, № 45, ст.400), всі програмно-апаратні комплекси повинні бути сертифіковані. Згідно з цим законом, сертифікація повинна відповідати вимогам, внесеним змінами і доповненнями до закону, зокрема, змінами, внесеними Законами № 440-IX від 14.01.2020, № 28 від 2020 року, № 1089-IX від 16.12.2020, № 1591-IX від 30.06.2021 та № 2801-IX від 01.12.2022.

За допомогою такої структури можливий короткий опис усіх основних моментів, пов'язаних з політикою безпеки організації, «не прив'язуючись» до конкретного технічного рішення, продукту чи виробника. В іншому випадку, при зміні політичної ситуації в компанії та інших факторах, може виникнути необхідність у зміні концепції ІБ, що бажано уникати. Також в політиці безпеки організації повинно бути чітке визначення обов'язків посадовців для розробки програм безпеки та впровадження їх в життя. Таким чином, політика безпеки є

основою підзвітності персоналу. До адміністративного рівня інформаційної безпеки відносяться загальні дії, які визначаються керівництвом підприємства.

Головна мета заходів на адміністративному рівні полягає в формуванні програми робіт в областях інформаційної безпеки і забезпечення її виконання, виділення необхідних ресурсів і контролі за станом справ. Основою програм є політики безпеки організації, які відображають підходи до захисту інформаційного активу.

Керівництво компанії повинне усвідомлювати необхідність підтримки режимів безпеки, виділення значних ресурсів на ці цілі, а також призначення відповідального за розробку, впровадження і супровід систем безпеки. Для «ЯВІР ДНІПРО-1» актуальним є створення політик інформаційної безпеки спільно з директором і кваліфікованим спеціалістом з кібербезпеки, які беруть на себе відповідальність за розробку, впровадження і вдосконалення системи безпеки.

2.2 Система виявлення і попередження вторгнень

2.2.1 Вибір програмного засобу виявлення і попередження вторгнень

Система виявлення вторгнень (СВВ, Intrusion Detection System (IDS)) – це програмний або апаратний засіб, який використовується в мережах для підвищення рівня захищеності інформаційних систем, центрів обробки цих систем, робочих станцій користувачів, серверів і комунікаційного обладнання, а також для виявлення фактів неавторизованого доступу в комп'ютерних систем або мережі, або несанкціонованого управління ними, головним чином через Інтернет.

Виявлення мережевих комп'ютерних атак (вторгнень) ґрунтується на аналізу мережевого трафіку стека протоколів TCP/IP. Обробка даних з метою виявлення вторгнень здійснюється методом сигнатурного і евристичного аналізу.

Рішення передбачається здійснити на базі комплексу програмних засобів захисту інформації, виробництва ТОВ «ТЕЛЕМАРТ». Вони пропонують кожній

організації індивідуальний підхід. У нашому випадку для розгортання захищеної мережі оптимальним варіантом є програмний пакет ViPNet Office Firewall версії 3.10. Дане ПЗ поставляється в комплектації Light, яка включає ліцензію на створення одночасно до двох координаторів, десяти абонентських пунктів, п'яти тунельних з'єднань. При необхідності можна докупити додаткові ліцензії при збільшенні кількості робочих станцій.

Програмний пакет ViPNet Office Firewall дозволяє розгорнути віртуальну мережу високої міри захищеності, не змінюючи існуючу фізичну інфраструктуру мережі і не знижуючи її продуктивність. У ViPNet Office Firewall будований ряд захищених інструментів, які дозволяють користувачам легко і ефективно взаємодіяти в мережі.

Перевага використання технології ViPNet полягає в забезпеченні цілісності усіх переданих даних і захисті мережі від зовнішніх і внутрішніх атак. Ці заходи безпеки здійснюються за допомогою програмних модулів ViPNet, встановлених на всіх комп'ютерах в мережі (включаючи робочі місця користувачів і сервери). ПЗ ViPNet повністю контролює TCP/IP трафік шляхом його шифрування і фільтрації відповідно до встановленої політикою безпеки.

В результаті, якщо будь-який комп'ютер зі встановленим ПЗ ViPNet, який знаходиться як в зовнішній мережі, так і в внутрішньому сегменті, з'єднується з іншим ViPNet-комп'ютером, то це з'єднання зашифроване (створює тунель) і ізольоване від зовнішніх мережевих з'єднань. Тунельне з'єднання, створюється поверх існуючих каналів Інтернет і шифрується за допомогою стійких криптографічних алгоритмів, тому його не можна перервати або перехопити.

Традиційні VPN-рішення зазвичай акцентують увагу на захисті трафіку між двома видаленими локальними мережами або між локальною мережею і видаленими (чи мобільними) користувачами. Технологія ViPNet забезпечує створення безпосереднього і захищеного з'єднання «клієнт-клієнт». Крім того, у всі компоненти ViPNet Office Firewall інтегровані модулі IDS (Intrusion Detection System - система виявлення атак) і міжмережевий екран, тому ViPNet успішно

забезпечує захист трафіку як між видаленими мережами, так і всередині локальної мережі.

Ядром програмного забезпечення ViPNet є так званий ViPNet Драйвер, основною функцією якого є фільтрація і шифрування/дешифрування вхідних і вихідних IP-пакетів.

Кожен вихідний пакет обробляється драйвером відповідно до одного з наступних правил:

- переадресовується або вирушає в початковому вигляді (без шифрування);
- блокується;
- шифрується і вирушає;
- шифрується і переадресовується.

Кожен пакет, що входить, обробляється таким чином:

- пропускається (якщо він не зашифрований і це дозволено правилами фільтрації для нешифрованого трафіку);
- блокується (відповідно до встановлених правил фільтрації);
- розшифровується (якщо пакет був зашифрований) і перенаправляється для подальшої обробки відповідним застосуванням.

ViPNet Драйвер працює між канальним та мережевим рівнем моделі OSI, що дозволяє обробляти IP-пакети до їх подальшої обробки стеком протоколів TCP/IP та передані на прикладний рівень. Таким чином, ViPNet Драйвер захищає IP-трафік усіх застосунків, не порушуючи звичний порядок роботи користувачів. Графічне зображення ViPNet Драйвера в моделі OSI представлено на рис. 2.3.

Внаслідок такого підходу впровадження технології ViPNet не вимагає зміни складених бізнес-процесів, а витрати на розгортання мережі ViPNet є невеликими. Наступна схема ілюструє роботу Відповідного Драйвера ViPNet під час обробки запиту на перегляд веб-сторінки, яка розміщена на IIS-сервері, що функціонує на Комп'ютері Б. Графічна схема роботи двох комп'ютерів у мережі, захищених ПЗ ViPNet представлена на рис. 2.4.

Комп’ютер А відправляє запит до Комп’ютера Б за допомогою протоколу HTTP. Запит передається на нижні рівні стеку TCP/IP, і на кожному рівні до нього додається службова інформація.

Рисунок 2.3 - ViPNet Драйвер в моделі ISO

Коли запит досягає ViPNet Драйвера, Драйвер зашифровує його і додає свою власну інформацію. ViPNet Драйвер, працюючий на Комп’ютері В, приймає запит, видаляє з нього службову інформацію ViPNet, розшифровує запит і передає по стеку TCP/IP на прикладний рівень для подальшої обробки.

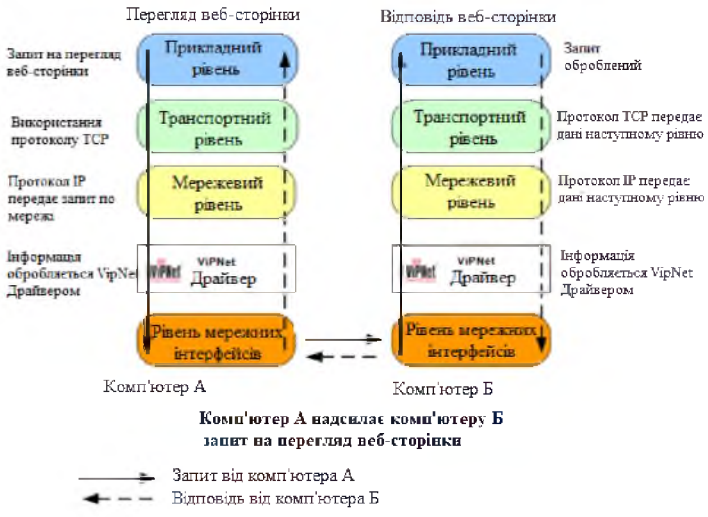


Рисунок 2.4 - Схема роботи мережі TCP/IP. захищеною ПЗ ViPNet

У технології ViPNet для шифрування використовується комбінація криптографічних алгоритмів із симетричними та асиметричними ключами, які представлені в таблиці 2.1.

Таблиця 2.1 - Застосування криптографічних алгоритмів в ПЗ ViPNet

Криптографічні алгоритми	
З симетричними ключами	**З асиметричними ключами**
- шифрування IP-трафіка - шифрування повідомлень «Ділової пошти» - шифрування прикладних і службових конвертів	- створення і перевірка ЕЦП - шифрування в сторонніх застосуваннях за допомогою криптопровайдера ViPNet

В ПЗ ViPNet для шифрування використовуються наступні симетричні алгоритми: ДСТУ 28147:2020 (з довжиною ключа 256 біт) - стандарт симетричного шифрування, та AES (256 біт) - прийнятий у США стандарт симетричного шифрування, розроблений на основі алгоритму Rijndael.

За умовчанням використовується алгоритм ДСТУ 28147:2009. У разі необхідності можна вибрати алгоритм AES.

2.2.2 Модулі програми ViPNet Office Firewall

Програма ViPNet Office Firewall складається з наступних модулів:

- Низькорівневий драйвер мережевого захисту ViPNet Драйвер: цей драйвер взаємодіє безпосередньо з драйверами мережевих інтерфейсів і контролює весь IP-трафік, що проходить через них.

- Програми Монітора: цей модуль надає інтерфейс користувача для різних налаштувань Драйвера та фіксує всі необхідні події в спеціальних журналах реєстрації IP-трафіка.

- Програми Контроль Додатків: цей модуль здійснює захист від несанкціонованих спроб додатків виконати мережеву операцію.

Цей комплекс пройшов сертифікацію в Міністерстві економічного розвитку і торгівлі України та на даний момент має сертифікат відповідності від

державної система сертифікації УкрСЕПРО № ВГ UA1.066.037979-16 (Додаток Г).

Даний сертифікат підтверджує, що виріб «Програмний комплекс» «ViPNet Office Firewall» у відповідності до формуляру відповідає вимогам ДСТУ 28147 і вимогам України до засобів криптографічного захисту інформації класу КСЗ. Виріб може використовуватися для криптографічного захисту (шифрування файлів, даних, що містяться в областях оперативної пам'яті, і IP-трафіка: обчислення для файлів, даних тих, що містяться в оперативній пам'яті та IP-трафіка). Важливо відзначити, що ця інформація не містить відомостей, які становлять державну таємницю.

Сертифікат виданий на підставі результатів сертифікаційних випробувань зразка продукції № 486А-001001, проведених товариством з обмеженою відповідальністю «Центр сертифікаційних досліджень».

Цей сертифікат засвідчує, що програмний комплекс захисту інформації «ViPNet Office Firewall», є програмним засобом захисту інформації від несанкціонованого доступу, відповідає вимогам керівних документів, зокрема Наказу від 22.12.2008 № 495 «Про прийняття міждержавних стандартів як національні методом підтвердження та скасування відповідних міждержавних стандартів «Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» (ДСТУ 28147:2009) - до 3 класу захищеності та «Захист від несанкціонованого доступу до інформації. Частина 1. Програмне забезпечення засобів захисту інформації. Класифікація за рівнем контролю відсутності можливостей», яке не декларується, - по 3 рівню контролю і технічних умов.

Крім того, цей комплекс може використовуватися при створенні автоматизованих систем класу захищеності до IP включно і для захисту інформації в інформаційних системах персональних даних до 1 класу включно.

Розглянемо кожен компонент детальніше:

1. ViPNet Manager

Програму ViPNet Manager слід встановлювати на спеціально виділеному робочому місці адміністратора перед встановленням інших компонентів пакету ViPNet Office Firewall.

ViPNet Manager відповідає за створення логічної структури мережі ViPNet, включаючи зв'язки між серверами та робочими місцями користувачів, а також за генерацію наборів ключів і паролів для кожного мережевого вузла. Набори ключів використовуються для встановлення захищених з'єднань і обов'язкові для установки на мережеві вузли, які використовують ПЗ ViPNet Coordinator і ViPNet Client.

Комп'ютер з встановленою програмою ViPNet Manager не обов'язково має бути постійно доступний в мережі, оскільки ViPNet Manager використовується переважно для створення початкової структури мережі і генерації ключових наборів, а після цього - для періодичного обслуговування мережі. Для того щоб адміністратор мережі ViPNet міг встановлювати з'єднання з іншими мережевими вузлами ViPNet і розсилати набори ключів, на робочому місці адміністратора повинно бути встановлено ПЗ ViPNet Client (у програмі ViPNet Manager мережевий вузол, який є робочим місцем адміністратора, відзначений значком).

До складу ViPNet Manager входить майстер «Створення мережі ViPNet», який допомагає пройти всі етапи створення мережі ViPNet. Цей майстер має дружній інтерфейс і значно полегшує створення мережі вперше.

У програмі ViPNet Manager також передбачена можливість створювати резервні копії конфігурації мережі, а також виконувати віддалене оновлення ПЗ ViPNet на мережевих вузлах.

У ViPNet Manager можна встановлювати рівні повноважень для користувачів мережі ViPNet. Рівень повноважень визначає можливості користувача щодо зміни налаштувань встановленого ПЗ ViPNet. За умовчанням встановлений стандартний рівень повноважень.

Крім того, програма ViPNet Manager надає можливість організувати захищену міжмережеву взаємодію своєї мережі з іншими мережами ViPNet (наприклад, декілька офісів або віддалених користувачів).

2. ViPNet Coordinator

Комп'ютер з встановленим на ньому програмним забезпеченням ViPNet Coordinator вважається координатором і виконує одну з центральних ролей в мережі ViPNet. Однією з ключових функцій координатора є роль сервера IP-адрес. Кожен клієнт у мережі підключається до призначеного йому координатора, повідомляє йому свій поточний IP-адрес, і у відповідно отримує адреси інших активних мережевих вузлів на даний момент.

Коли координатор отримує інформацію про IP-адреси активних клієнтів, зареєстрованих на інших координаторах, він розсилає цю інформацію всім своїм клієнтам. У випадку, якщо координатор не отримує дані від якого-небудь клієнта протягом заданого проміжку часу (за замовчуванням 5 хвилин), він вважає, що цей клієнт неактивний і розсилає інформацію про статус клієнта іншим підключеним мережевим вузлам.

Після отримання клієнтами від своїх координаторів інформації про статус один одного, вони можуть встановлювати прямі з'єднання між собою. Ця можливість розповсюджується на всі онлайн-сервіси пакету ViPNet Office Firewall.

Іншою важливою функцією координатора є функція міжмережевого екрану для шифрованих з'єднань. Ця функція дозволяє:

- Декільком ViPNet-клієнтам, які працюють в локальній мережі через ViPNet-координатор, надається можливість використовувати один зовнішній IP-адрес.

- Тунелювання трафіку від комп'ютерів локальної мережі, які не мають програмного забезпечення ViPNet, до інших об'єктів мережі VPN (координатор може виконувати функції сервера, що тунелює, якщо немає необхідності захищати трафік окремого мережевого вузла або виконувати криптографічну аутентифікацію вузла усередині локальної мережі).

- Перемаршрутизація зашифрованого трафік ViPNet-клієнтів на адресу їхнього координатора (здійснюється підміна IP і MAC-адреси), а також прокладання через міжмережеві екрани (брандмауери, Firewall) інших типів.

Координатор також може виконувати функцію класичного міжмережевого екрану Firewall, який реалізує встановлені правила фільтрації та політику безпеки для відкритого трафіку. Якщо клієнт працює через координатор, який виконує трансляцію адрес (NAT - Network Address Translation) для шифрованого трафіку, то весь шифрований трафік маршрутизується через координатор.

При цьому координатор не обробляє нешифрований (відкритий) трафік клієнтів. Відкритий трафік обробляється звичайним способом відповідно до конфігурації операційної системи клієнта і правил маршрутизації відкритого трафіку, прийнятих в мережі.

Важливою функцією координатора є забезпечення трансляції відкритих мережевих адрес NAT. Можна налаштувати статичні та динамічні правила трансляції для підключення до відкритих ресурсів Інтернету.

Координатор також підтримує трансляцію мережевих адрес на прикладному рівні для протоколу FTP, що забезпечує можливість роботи FTP-клієнтів в активному режимі, а також фільтрацію команд протоколу FTP для захисту від використання некоректних значень IP-адрес клієнта і сервера. Налаштування координатора та контроль його роботи здійснюються за допомогою програми ViPNet Coordinator [Монітор].

3. ViPNet Client

Програма ViPNet Client має бути встановлена на робочих місцях користувачів мережі ViPNet. Завдяки простоті установки, автоматичному визначенню мережевих налаштувань, набору передвстановлених рівнів мережевої безпеки і інтуїтивно зрозумілому інтерфейсу, навіть недосвідчені користувачі можуть легко працювати з програмою ViPNet Client.

ViPNet Client включає:

- Інтегрований персональний мережевий екран з функціями виявлення атак IDS і контролю мережевої активності додатків;

- TCP IP шифратор;

- Ряд корисних захищених комунікаційних застосувань і інших функцій.

Одна з найважливіших функцій ПЗ ViPNet Client - ефективний контроль IP-трафіку під час завантаження операційної системи (ОС). Цей контроль здійснюється завдяки безпосередній взаємодії між ViPNet Драйвером і драйверами мережевих адаптерів. У ОС Windows для ініціалізації завантаження комп'ютера використовує тільки одна служба. Ініціалізація ViPNet Драйвера і ключів шифрування ViPNet виконується перед входом користувача в Windows, тобто до ініціалізації інших служб і драйверів операційної системи.

В результаті, ViPNet Драйвер першим отримує контроль над стеком протоколів TCP/IP. До моменту ініціалізації драйверів мережевих адаптерів, ViPNet Драйвер готовий до шифрування і фільтрації трафіку, забезпечуючи захищене з'єднання з контролером домена, контроль мережевої активності запущених на комп'ютері застосунків і блокування небажаних пакетів із зовнішнього середовища. Під час завантаження операційної системи, ПЗ ViPNet перевіряє власні контрольні суми, що гарантує цілісність програмного забезпечення, наборів ключів і списку додатків, яким дозволена мережева активність.

При перегляді інтернет-ресурсів, ViPNet Client забезпечує:

- Блокування найбільш поширених банерів та рекламних спливаючих вікон, які можуть відволікати користувача та призводити до збільшення інтернет-трафіку. Список блокованих банерів може бути розширений за потреби.

- Блокування різних інтерактивних елементів, таких як ActiveX, Java-додатки, Flash-анімація, сценарії JavaScript і VBScript, які можуть виконувати несанкціоновані дії користувачем.

- Захист від несанкціонованого збору інформації про дії користувача в Інтернеті, шляхом блокування використання Cookie і Referer.

Можна задати загальні правила фільтрації вмісту для всіх веб-сайтів та включити окремі веб-сайти в список виключень за допомогою ViPNet Client. Це ПЗ дозволяє управляти параметрами обробки прикладних протоколів FTP, HTTP і SIP.

Програмне забезпечення ViPNet Client може бути встановлене для захисту трафіку на будь-якому комп'ютері з ОС Windows, будь то стаціонарний комп'ютер, віддалений або мобільний комп'ютер, або сервер.

Налаштування та управління роботою клієнта здійснюється за допомогою програми ViPNet Client [Монітор].

4. ViPNet IDS

Метод сигнатурного аналізу базується на використанні набору правил виявлення атак (вторгнень), які передбачено в ViPNet IDS та регулярно оновлюються. Паралельно з сигнатурним аналізом може використовуватися евристичний аналіз для виявлення аномалій у мережевому трафіку.

При виявленні комп'ютерної атаки (вторгнення) ViPNet IDS реєструє факт виявлення атаки (вторгнення), ідентифікує подію і сповіщає адміністратора через веб-інтерфейс ViPNet IDS. Це дає можливість швидко скоригувати налаштування безпеки мережі або виявити слабкі місця в системі безпеки. При необхідності адміністратор може налаштувати повідомлення про виявлені атаки (вторгненнях) по електронній пошті

У пасивній IDS при виявленні порушення безпеки інформація про порушення записується у журнал додатка, а також сигнали небезпеки передаються на консоль і/або адміністраторові системи через визначений канал зв'язку. У випадку активної системи, відомої як система запобігання вторгнень (IPS - Intrusion Prevention System), IDS вживає заходів у відповідь на порушення, таких як скидання з'єднання або перенастроювання міжмережевого екрана для блокування трафіку від зловмисника. Дії у відповідь можуть виконуватися автоматично або за командою оператора.

2.2.2 Додаткові додатки ViPNet Office Firewall

Пакет ViPNet Office Firewall включає ряд корисних застосувань для швидкого і безпечного обміну даними між учасниками мережі ViPNet, а також інші функції:

1. Обмін захищеними повідомленнями Захищена конференція.

Ця функція призначена для передачі повідомлень між користувачами мережі ViPNet в реальному масштабі часу. Додаток порівнюється з іншими інструментами, такими як ICQ, MSN Messenger, AOL Instant Messenger, Skype, Telegram, Viber, Facebook Messenger, WhatsApp, IRC, Signal. Проте перевагою ViPNet є те, що усі повідомлення шифруються в реальному часі, забезпечуючи високий рівень конфіденційності і безпеки обміну інформацією.

2. Ділова пошта.

Це поштовий клієнт із потужною системою верифікації та аутентифікації, яка перевершує можливості звичайних поштових програм. Програма дозволяє відстежувати статус повідомлень (відправлено, доставлено, прочитано), підтверджувати особу відправника за допомогою ЕЦП (електронному цифровому підпису), використовуючи систему сертифікатів користувачів, що вбудована в загальну систему безпеки. Інтерфейс додатка призначений для користувача і відповідає загальноприйнятим стандартам для подібних поштових програм.

3. Файловий обмін.

Функція дозволяє швидко і зручно обмінюватися файлами з іншими користувачами ViPNet, не потребуючи налаштування додаткових служб чи програм (наприклад, спільного доступу до ресурсів або FTP-сервера). Вона інтегрована в оболонку Windows Explorer і може бути викликана з контекстного меню. Розмір переданих файлів не обмежений.

4. Виклик зовнішніх застосувань.

ViPNet підтримує автоматизований захищений обмін даними для ряду комунікаційних застосувань, таких як MS NetMeeting, VoxPhone, Internet Phone, Compaq Insight Manager, Microsoft Portrait, Radmin Viewer, з забезпеченням примусового шифрування трафіку цих застосувань. Крім того, ви можете використати будь-які інші комунікаційні застосування, що передають дані по протоколу TCP/IP. Однак для гарантованого захисту трафіку цих застосувань важливо переконатися, що їх маршрутизація здійснюється в межах мережі ViPNet.

5. Відкрити веб-ресурс мережевого вузла.

Функція дозволяє звертатися до веб-ресурсів на комп'ютері з встановленим програмним забезпеченням ViPNet. З'єднання з вузлами ViPNet відбувається в захищеному режимі.

6. Огляд загальних ресурсів мережевого вузла.

Функція дозволяє відкривати загальні мережеві ресурси на комп'ютері з встановленим програмним забезпеченням ViPNet. З'єднання з вузлами ViPNet відбувається в захищеному режимі.

2.3 Вибір апаратної платформи для реалізації правил виявлення мережевих атак

В якості апаратної платформи для варіанту виконання: IDS 2000 Q2 (далі – IDS 2000 Q2) використовується сервер AquaServer T50 D14 виробництва ГК «Акваріус». Рис. 2.5 представлена передня панель IDS 2000 Q2.

Рисунок 2.5 - Передня панель IDS 2000 Q2

IDS 2000 Q2 має наступні технічні характеристики, представлені в таб. 2.2:

Таблиця 2.2 - Характеристики IDS 2000 Q2

Характеристика	**Опис**
Форм-фактор	Сервер AquaServer T50 D14 19" Rack 1U
Розміри (ШхВхГ)	444x43x685 мм
Маса	15 кг
Живлення	Вбудований блок живлення потужністю 600 Вт, 110-220 В
Споживана потужність	470 Вт
Процесор	2xIntel Xeon E5 - 2620v2
Оперативна пам'ять	Від 16 ГБ
Характеристика	Опис
Мережеві порти	4 порту Ethernet RJ45 10/100/1000 Мбіт/с 2 порти Ethernet SFP+ 10 Гбіт/с
Порти введення-виводу	VGA PS/2 Клавіатура, PS/2 Миша 1 COM -порт RS - 232 4 порти USB 2.0

На передній панелі IDS 2000 Q2 розташовані 2 роз'єми USB, інші комунікаційні роз'єми знаходяться на задній панелі рис. 2.6.

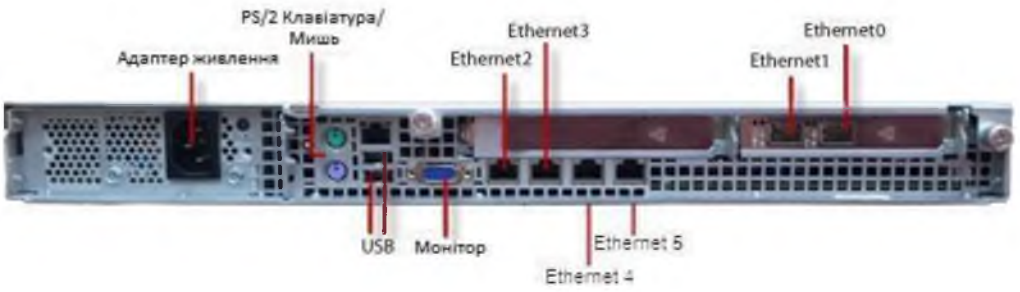


Рисунок. 2.6 - Задня панель IDS 2000 Q2

Можливості IDS 2000 Q2 з використанням програмної платформи ViPNet IDS:

1. Евристичний метод виявлення аномалій мережевого трафіку дозволяє збирати статистичну інформацію про параметри мережевого трафіку протягом певного періоду. На основі цих даних він будує еталон мережевого трафіку, в якому визначені максимальні та мінімальні значення параметрів трафіку за певний період. У випадку відхилення поточного трафіку від цих еталонних значень, адміністратор отримує сповіщення, що дозволяє йому прийняти заходи для блокування атак на основі конкретних параметрів трафіку;

2. Евристичний метод виявлення аномалій в поведінці користувачів ViPNet IDS дозволяє виявити нетиповий час входу/виходу в ViPNet IDS або перевищення звичайної частоти входу/виходу в ViPNet IDS;

3. Виявлення атак на канальному рівні. ViPNet IDS дозволяє виявляти атаки на нижчому, канальному рівні, такі як ARP – spoofing;

4. Ролева модель реалізована в ViPNet IDS, що дозволяє розмежовувати повноваження користувачів з управління ViPNet IDS;

5. Відновлення властивостей ViPNet IDS після збоїв забезпечується механізмом резервування основних компонентів ViPNet IDS;

6. Аудит безпеки ViPNet IDS. Дозволяє виконувати відстеження та реєстрацію подій у журналах функцій ViPNet IDS. Ця можливість надає

адміністраторові змогу контролювати значущі зміни в налаштуваннях ViPNet IDS;

7. Самотестування ViPNet IDS. Дозволяє контролювати цілісність та незмінність основних компонентів ViPNet IDS. Крім того, ця функція робить перевірку на наступних аспектів:

- збіг контрольних сум основних конфігураційних файлів;

- відповідність апаратної платформи ViPNet IDS бінарному коду ПЗ ViPNet IDS;

- наявність завантаженої ліцензії і її підпису;

- достовірність завантажених правил виявлення атак.

У разі виникнення помилок цілісності адміністратори ViPNet IDS повідомляються про несправності системи;

8. Паролі облікових записів користувачів ViPNet IDS. Додана автоматична перевірка паролів користувачів на відповідність вимогам по безпеці паролів в ViPNet IDS;

9. Покращений веб-інтерфейс управління ViPNet IDS.

Програмно-апаратний комплекс ViPNet IDS надає можливість:

1. Здійснювати автоматичний аналіз та виявлення комп'ютерних атак (вторгнень) на основі динамічного аналізу мережевого трафіку стека протоколів TCP/IP для протоколів на всіх рівнях моделі взаємодії відкритих систем, починаючи з канального і закінчуючи прикладним рівнем;

2. Проводити евристичний аналіз для виявленню аномалій в мережевому трафіку та діях користувачів ViPNet IDS;

3. Аналізувати мережевий трафік у режимі, близькому до реального масштабу часу;

4. Аналізувати мережевий трафік, що надходить одночасно з декількох мережевих інтерфейсів;

5. Виявляти вторгнення на основі аналізу службової інформації протоколів мережевого рівня;

6. Журналювати виявлені події та атаки (вторгнення) для подальшого аналізу;

7. Відображати виявлені атаки (вторгнення) у веб-інтерфейсі ViPNet IDS та повідомляти адміністратора про виявлені атаки по електронній пошті;

8. Відображати узагальнену статистичну інформацію про атаки;

9. Здійснювати вибірковий пошук подій і атак (вторгнень) відповідно до заданих фільтрів;

10. Експортувати журнали атак (вторгнень) у файл формату CSV для подальшого аналізу в сторонніх застосуваннях;

11. Реєструвати, відображати та експортувати у файл формату PCAP IP-пакети, що відповідають зареєстрованим атакам (вторгненням);

12. Оновлювати бази вирішальних правил в автоматизованому режимі при надходженні нової версії вказаної бази виробником;

13. Додавати власні правила для аналізу мережевого трафіку;

14. Вибірково використати окремі правила виявлення або групи правил.

Цей програмно-апаратний комплекс повністю відповідає заданим вимогам, завдяки можливості гнучкого налаштування, двом видам аналізу і можливістю оновлення баз правил.

Для виявлення атак в мережевому трафіку використовується метод сигнатурного аналізу, який базується на використанні правил виявлення атак, заздалегідь передбачених у ViPNet IDS та завантажених заздалегідь. На основі цих правил ViPNet IDS приймає рішення щодо вмісту атак у трафіку.

Схема взаємодії компонентів ViPNet IDS під час аналізу мережевого трафіку сигнатурним методом (на основі правил виявлення атак) представлена на рис. 2.7.

Обробка трафіку за допомогою ViPNet IDS здійснюється в наступній послідовності:

1. Трафік, який відображається SPAN-портом на ViPNet IDS, обробляється Сенсором. Сенсор перехоплює та розподіляє мережевий трафік між модулями виявлення атак. Після цього мережевий трафік аналізується модулями виявлення

на основі правил виявлення атак. Після аналізу Сенсор зберігає результати аналізу мережевого трафіку і передає їх на Сервер. Результати аналізу також кешуються на жорсткому диску, що забезпечує їх збереження при перезавантаженні ViPNet IDS.

Рисунок 2.7 - Схема взаємодії компонентів ПЗ ViPNet IDS

2. Сервер декодує результати аналізу мережевого трафіку в спеціальний текстовий формат, який підтримується модулем завантаження, і зберігає їх на жорсткий диск. При необхідності Сервер може передавати отримані дані зовнішньому сторонньому ПЗ.

3. Модуль завантаження даних у БД PostgreSQL завантажує дані з кеша Сервера і передає їх у базу даних PostgreSQL.

4. Для відображення отриманої інформації про мережеві атаки (вторгнення) використовується веб-інтерфейс ViPNet IDS.

5. При використанні системи моніторингу ViPNet StateWatcher модуль взаємодії з ViPNet StateWatcher підключається до БД PostgreSQL і передає дані про наявність виявлених мережевих атаках (вторгненнях) системі моніторингу.

У ViPNet IDS реалізований два евристичні методи:

1. Евристичний метод виявлення аномалій мережевого трафіку.

2. Евристичний метод виявлення аномалій поведінки користувачів ViPNet IDS.

Обидва ці методи можуть використовуватися додатково до сигнатурного аналізу. Залежно від вашого вибору, ви можете відмовитися від використання евристичних методів або налаштувати їх за власним бажанням.

Принцип роботи евристичного методу виявлення аномалій мережевого трафіку в ViPNet IDS базується на основному сигнатурному методі виявлення атак. Однак рекомендується додатково використовувати евристичний метод для виявлення аномалій в мережевому трафіку. Цей метод дозволяє відстежувати трафік протягом певного періоду і на основі математичних алгоритмів створювати еталон мережевого трафіку.

Суть використання евристичного методу полягає в постійному моніторингу мережевого трафіку в режимі реального часу і перевірці того, чи параметри трафіку виходять за межі прогнозованих значень. Всі випадки відхилення фіксуються і автоматично повідомляються адміністратору. На основі цих даних адміністратор може прийняти рішення про зміну налаштувань міжмережевого екрану для блокування певних типів атак.

Комбінація двох методів (сигнатурного і евристичного) забезпечує більш комплексний захист від усіх типів загроз. Для виявлення аномалій мережевого трафіку евристичним методом в ViPNet IDS використовуються відповідні евристичні модулі. Кожному модулю виявлення атак відповідає свій евристичний модуль. Це реалізовано для розпаралелювання обробки мережевого трафіку, де кожен модуль виявлення атак і його відповідний евристичний модуль обробляють окремі частини мережевого трафіку.

Під час роботи евристичні модулі періодично (за умовчанням, раз в 10 хвилин) зберігають інформацію про параметри мережевого трафіку за вказаний інтервал часу у відповідних журналах статистики.

2.4 Платформа розвідки загроз Threat intelligence

Threat Intelligence – це інформація, що охоплює процес її отримання та надає відомості про загрози і порушників. Ця інформація розкриває методи, які використовують зловмисники для завдання шкоди, а також способи протидії їм.

Система Threat Intelligence дозволяє проводити швидший і найефективніший аналіз шкідливого коду та генерувати додаткові ідеї для його усунення.

Ця система працює не лише і не стільки зі статичною інформацією про окремі вразливості та загрози, скільки з більш динамічною інформацією, яка має практичне значення. Вона включає в себе дані про джерела загроз, ознаки компрометації (що об'єднують різні відомості в єдине ціле), а також інформацію про шкідливі домени і IP-адреси, взаємозв'язки та інші аспекти.

Threat Intelligence розділяється на дві категорії: оперативний пошук шкідливого коду, протиправних дій і тому подібного, а також стратегічний пошук, який виконується людськими аналітиками.

Оперативна розвідка виконується виключно комп'ютерами, які відповідають за ідентифікацію та збір даних, що подальше збагачення та аналізуються. Типовим прикладом оперативного аналізу загроз є автоматичне виявлення розподіленої відмови в обслуговуванні (DDoS) атак. У цьому випадку порівняння між показниками компромісу та мережевою телеметрією використовується для ідентифікації атаки значно швидше, ніж може зробити людський аналітик.

Стратегічна розвідка фокусується на значно складнішому і обширнішому процесі виявлення і аналізу загроз основних активів організації, включаючи співробітників, клієнтів, інфраструктуру, додатки і постачальників. Для досягнення цієї мети висококваліфіковані людські аналітики повинні розвивати зовнішні зв'язки і власні джерела інформації, виявляти тенденції, навчати співробітників і клієнтів, вивчати тактики, методи і процедури зловмисників та, кінець-кінцем, робити рекомендації щодо оборонної архітектури для боротьби з ідентифікованими загрозами.

Програмно-апаратний комплекс ViPNet Threat Intelligence Analytics System використовується для автоматичного виявлення комп'ютерних атак та інцидентів на основі подій інформаційної безпеки з різних джерел. Основним джерелом подій інформаційної безпеки для ViPNet TIAS є ViPNet IDS, який аналізує мережевий трафік, що входить і виходить, за допомогою баз

вирішальних правил Snort IDS, розроблених компанією ТОВ "ТЕЛЕМАРТ". Деякі сигнатури написані для виявлення використання вразливостей. Після виявлення інцидентів ІБ програмно-апаратний комплекс ViPNet TIAS створює або змінює картку інциденту. У цій картці автоматично вказується вся інформація, пов'язана з вразливістю: клас інциденту, ознаки інциденту, залучені активи, критичність і методи ліквідації негативного впливу. Приклад картки інциденту представлений рис. 2.8.

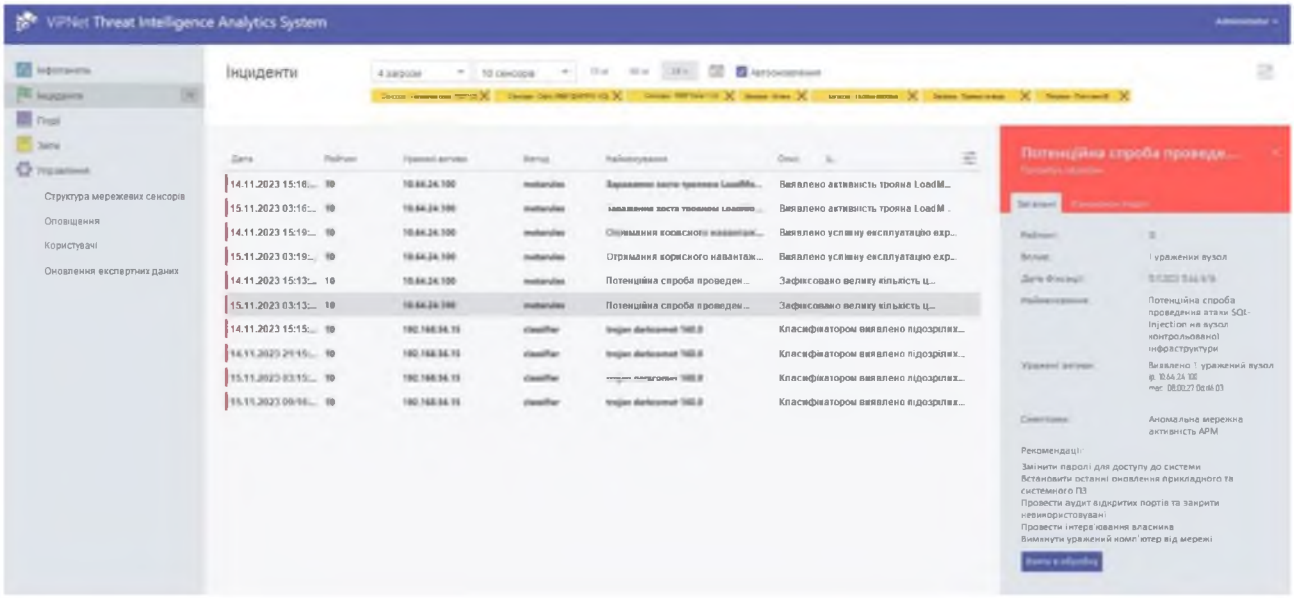


Рисунок 2.8 - Приклад картки інциденту

Програмно-апаратний комплекс ViPNet Coordinator HW1000 призначений для організації захищеного доступу до інфраструктури організації. Для видаленого управління IDS, ViPNet Coordinator HW1000 виступатиме в якості VPN-шлюза. Координатори в ролі VPN-шлюзів дозволяють захистити з'єднання між вузлами локальних мереж, які обмінюються інформацією через публічні мережі. Захист реалізується за допомогою технології тунелювання, в основі якої лежить інкапсуляція і шифрування того, що проходить через координатори трафіку. При цьому координатор може виконувати тунелювання як на мережевому рівні (рівень 3 моделі OSI), так і на канальному рівні (рівень 2 моделі OSI).

Тунелювання трафіку на мережевому рівні дозволяє створити захищене з'єднання між відкритим вузлом і захищеним вузлом ViPNet або між двома відкритими вузлами, які тунелюються різними координаторами. Це дозволяє інтегрувати відкриті вузли в захищену мережу ViPNet без необхідності встановлення на них програмного забезпечення ViPNet.

1. На координатор поступають відкриті IP-пакети від тунелюючих вузлів, які обробляються мережевими фільтрами.

2. Оброблені IP-пакети на координаторові шифруються і упаковуються в нові IP-пакет, після чого передаються на захищені вузли-одержувачі або на інший координатор.

3. Якщо на координатор надходить зашифрований IP-пакет, призначений для тунелюючих вузлів, з нього витягаються початкові IP-пакети, розшифровуються, проходять обробку мережевими фільтрами і подаються на вузли-одержувачі у відкритому вигляді.

Основні характеристики ViPNet Coordinator HW1000 табл. 2.3 і зображення задньої панелі рис. 2.9 представлено нижче.

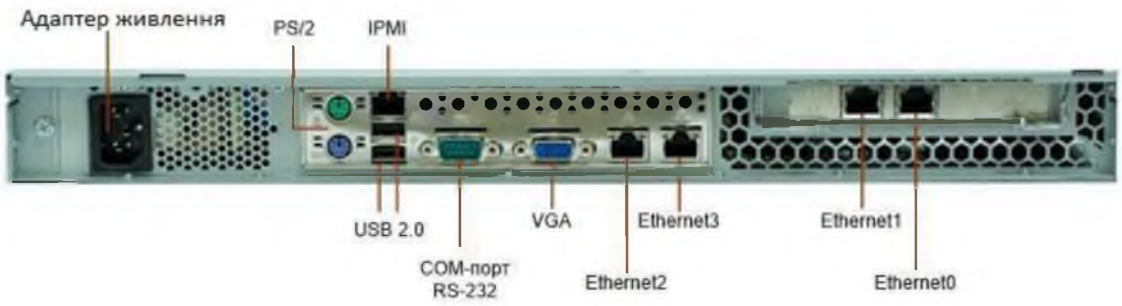


Рисунок 2.9 - Задня панель ViPNet Coordinator HW1000

ViPNet Coordinator HW1000 дозволяє безпечно управляти програмно-апаратними комплексами IDS, навіть без безпосереднього доступу до нього. Це особливо актуально в тих випадках, коли оператор знаходиться за межами локальної мережі організації. Такий підхід сприяє підвищенню швидкості реакції на інциденти і зменшенню критичності проведених атак для інформаційних ресурсів підприємства.

Таблиця 2.3 - Основні характеристики ViPNet Coordinator HW1000

Характеристика	Опис
Форм-фактор	Сервер AquaServer T40 S44 19" Rack 1U
Розміри (ШхВхГ)	432x43, 6x375 мм
Маса	6,5 кг
Живлення	Вбудований блок живлення потужністю 220 Вт, 110-220 В
Споживана потужність	До 155 Вт
Процесор	Intel Core i5 - 750
Оперативна пам'ять	Від 2 Гбайт
Мережеві порти	4 порту Ethernet RJ45 10/100/1000 Мбіт/с
Порти введення-виводу	VGA PS/2 Клавіатура, PS/2 Миша COM -порт RS - 232 4 порту USB 2.0

2.5 Правила Snort IDS

Правила Snort IDS - це правила, написані на мові Snort, які використовуються для ефективного та швидкого виявлення будь-якої підозрілої мережевої активності. Це досягається шляхом порівняння виявленого шкідливого трафіку, що проходить по локальній мережі організації, з визначеними правилами. Для написання правил Snort використовується проста мова опису правил, яка має широкі можливості і велику гнучкість.

Як видно на рис. 2.10, прогнозування подальших дій не пов'язане з конкретною атакою; воно, за інших рівних умов, застосовується і до інших цільових атак, більшість ознак яких були виявлені під час кореляції.

Більшість правил в мові Snort записуються в один рядок. Однак в сучасних версіях також можна записати складне правило в декілька рядків, якщо останній рядок закінчується спеціальним символом «\». Кожне правило Snort складається з двох частин: заголовка та опцій. Заголовок правила включає дію, протокол, IP-адреси та маски для відправника та одержувача, а також номери їх портів. В опційній частині правила вказується повідомлення та те, які частини пакетів слід перевірити для визначення застосування визначених дій. Нижче наведений приклад простого Snort-правила:

```
log tcp any any -> 192.168.1.0/24 111\
(content: \ "|00 08 90 g9|"; msg: "mountd access").
```

Це правило, при дотриманні усіх умов, записує інформацію про пакет в журнальний файл.

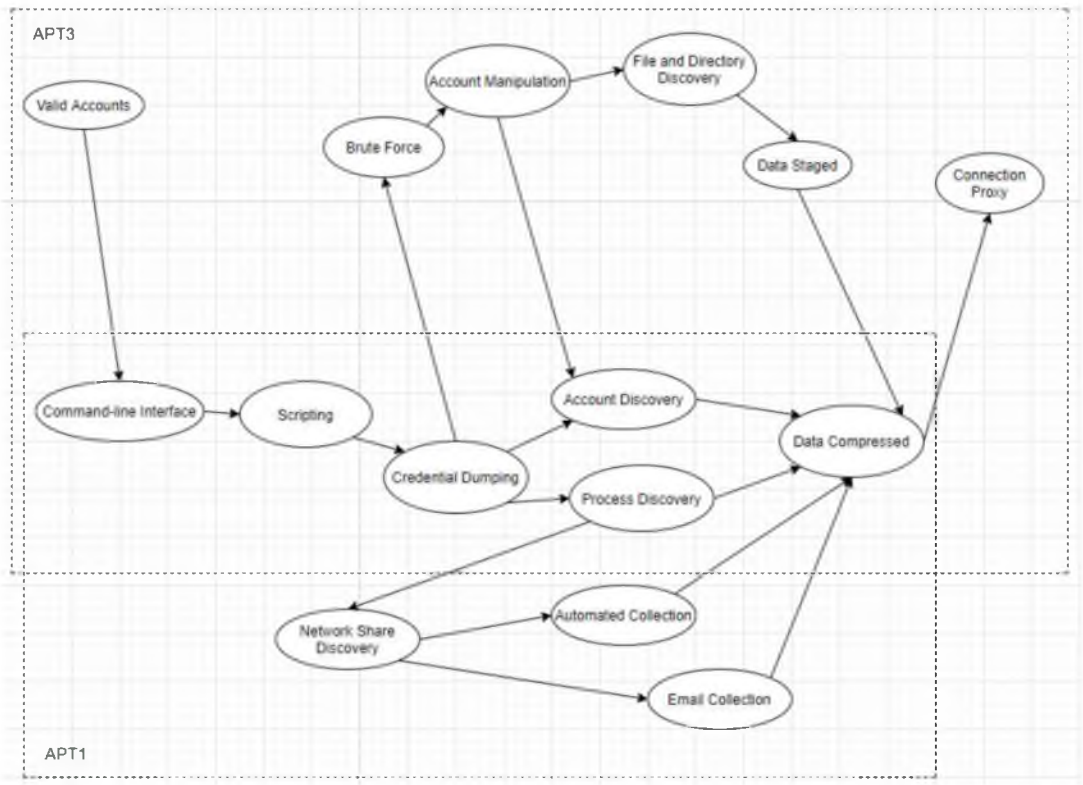


Рисунок 2.10 - Схемне представлення атак APT1 і APT3

В основі роботи інструментів виявлення та запобігання вторгненням (комп'ютерних атак) переважно лежить сигнатурний аналіз. Ефективність інструментів IDS напряму залежить від якості бази вирішальних правил (сигнатур), які вони застосовують. Якість цієї бази безпосередньо впливає на можливість виявлення атаки і визначає успішність роботи IDS. Існують два варіанти правил Snort IDS: купівля у виробників або використання безкоштовних правил. Розглянемо плюси і мінуси безкоштовних правил Snort IDS.

Однією з ключових переваг таких сигнатур є їх безкоштовність. Однак, вони мають певні недоліки:

1. Помилки синтаксису при написанні правил (якщо правило вказано неправильно, воно може не працювати або неправильно фільтрувати "корисні" пакети);

2. Логічні «закладки». При написанні деяких правил автори навмисно допускають помилки або включають спеціальні правила, щоб система не могла виявляти певні уразливості і типи атак;

3. Зміна політики ліцензування (закінчення надання безкоштовних оновлень для випущених баз правил, що може призвести до серйозних ускладнень у роботі системи);

4. Рідкісні і непостійні оновлення бази правил.

Структурно, модуль прогнозування є одним класом, який приймає на вхід підграф виявлених симптомів і порівнює їх з інформацією з файлу, в якому містяться ознаки APT-атак. На виході він повертає вектор, що складається з типів атак і варіантів розвитку атаки, що їм відповідають. UML-діаграма модуля прогнозування представлена на рис. 2.11.

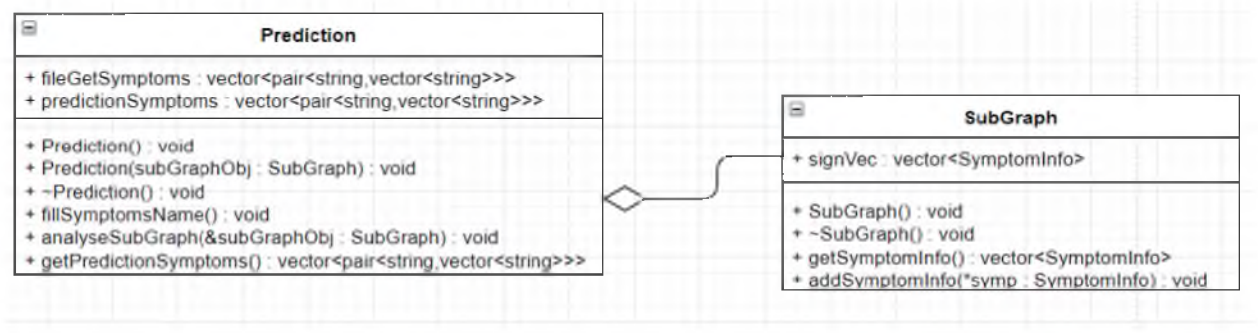


Рисунок 2.11 - UML-діаграма класів модуля прогнозування

Загальна схема модуля прогнозування представлена на малюнку 2.12.

В схемі вище видно, що модуль прогнозування, так само, як і інші модулі Snort IDS включається в основний модуль програми, куди він також повертає результат своєї роботи. З поданого вище можна зробити висновок, що база безкоштовних правил Snort IDS не підходить для компанії, які займаються обробкою персональних даних. Це обумовлено тим, що дані правила можуть бути уразливі або несвоєчасно виявляти підозрілу активність в локальній мережі компанії.

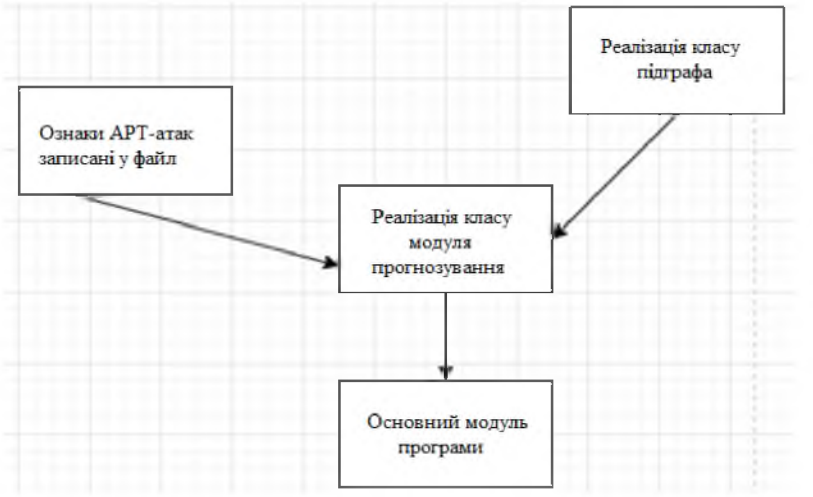


Рисунок 2.12 - Структурна схема модуля кореляції

Перевага і недоліки придбання правил Snort IDS у компанії ТОВ «ТЕЛЕМАРТ». Єдиним несуттєвим недоліком є те, що за ці правила, що надаються компанією ТОВ «ТЕЛЕМАРТ» треба сплачувати постійно. Незважаючи на це, база таких правил має велику кількість переваг:

1. Усі правила Snort IDS відповідають міжнародним стандартам і синтаксису мови Snort і детально описуються з їхніми функціями;

2. Кожен місяць розробляються 300-400 нових правил на основі щоденного аналізу більше шістдесяти тисяч зразків шкідливого коду і різних індикаторів компрометації;

3. Основні вирішальні правила тестуються на спеціальному стенді для виключення можливих неправдивих спрацьовувань і усунення помилок при написанні;

4. Простота установки і оновлення правил: не потрібно бути фахівцем і розбиратися в мові Snort, щоб встановлювати або оновлювати правила на обладнанні компанії.

Робота з правилами виявлення атак.

ViPNet IDS аналізує отриманий трафік для виявлення різних мережевих атак (вторгнень). Аналіз проводиться на основі правил, які встановлюються на ViPNet IDS при його введенні в експлуатацію. Для ViPNet IDS існують наступні типи правил:

1. Системні правила виявлення - правила, сформовані фахівцями ТОВ «ТЕЛЕМАРТ».

Перед введенням ViPNet IDS в експлуатацію необхідно завантажити і встановити системні правила виявлення атак з Сервера оновлень ТОВ «ТЕЛЕМАРТ». Оскільки мережеві атаки (вторгнення) постійно змінюються, рекомендується періодично оновлювати ці правила. Останні оновлення правил виявлення також розміщені на Сервері оновлень. Оновлення системних правил виявлення доступні лише за наявності діючої і тільки користувачеві з повноваженнями головного адміністратора.

2. Призначені для користувача правила виявлення - правила, створювані користувачами вручну.

Кількість призначених для користувача правил обмежена - на ViPNet IDS можна додати не більше 1000 власних правил. Створення призначених для користувача правил доступне тільки головному адміністратору.

Усі правила сортуються в групи відповідно від типу атак (вторгнень), до яких вони відносяться. Для призначених для користувача правил існує окрема група з назвою «local». Правила і групи правил можуть мати статуси «включено» або «вимкнено».

Головний адміністратор може виконувати наступні дії з правилами виявлення атак:

- встановлювати і оновлювати системні правила виявлення атак;

- змінювати статуси правил (включати або відключати правила виявлення атак);

- додавати, видаляти і редагувати власні правила виявлення атак.

Оскільки мережеві атаки (вторгнення) часто змінюються, необхідно постійно оновлювати правила виявлення з Сервера оновлень. Це дозволить вчасно виявляти найновіші типи атак (вторгнень).

Усі правила, встановлені на ViPNet IDS, розподілені по групах. Правила об'єднуються в групи за типом мережевих атак (вторгнень), що полегшує адміністраторові пошук необхідних правил. Щоб відключити або включити

правило, адміністратор спочатку вибирає групу, в якій знаходиться це правило, а потім встановлює або вимикає його. Системні правила виявлення атак неможливо видалити з ViPNet IDS; ви можете лише управляти їх статусами «включено» або «вимкнено».

Можна відключати як окремі правила (рис. 2.13), так і цілі групи правил (рис. 2.14). Після зміни статусів правил необхідно перезапустити ПЗ ViPNet IDS.

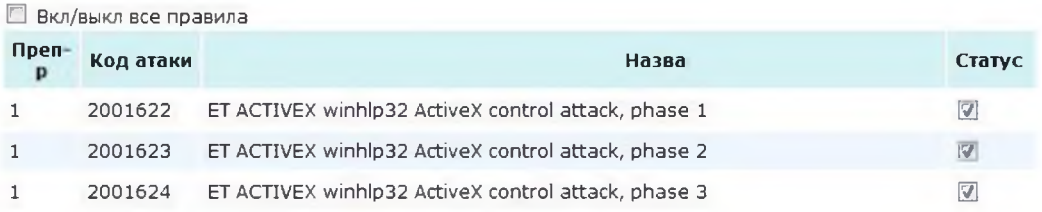


Рисунок 2.13 - Включення або виключення правил

ViPNet IDS надає можливість додавання власних правил виявлення атак. Усі призначені для користувача правила містяться у файлі local.rules. Для редагування, додавання і видалення призначених для користувача правил необхідно змінити файл local.rules, що розташований в каталозі /etc/snort/rules/, і потім завантажити його за допомогою веб-інтерфейсу ViPNet IDS.

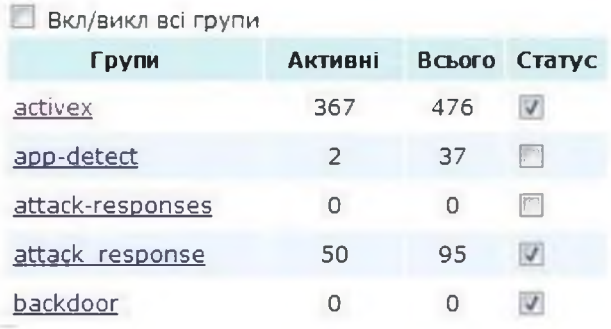


Рисунок. 2.14 - Включення або відключення групи правил

Після додавання призначених для користувача правил виявлення атак вони автоматично поміщаються в групу «local» і приймають статус «включено» або «вимкнено» залежно від налаштувань, заданих у файлі local.rules. Якщо правило

було закоментоване у файлі, то у веб-інтерфейсі ViPNet IDS воно буде відключено.

Щоб видалити усі призначені для користувача правила, необхідно завантажити порожній файл с назвою local.rules за допомогою веб-інтерфейсу.

2.6 Побудова системи виявлення, попередження і ліквідації наслідків комп'ютерних атак на базі мережі компанії «ЯВІР ДНІПРО-1»

Впровадження програмного комплексу ViPNet Office Firewall охопить усі структурні підрозділи підприємства, оскільки програма забезпечить повний контроль над усією локальною мережею, розгорнутою на підприємстві. Як було зазначено раніше, ViPNet Office Firewall включає комплекс із трьох програмних продуктів, кожен з яких встановлюється на ПК відповідно до виконуваної функції. Також, кожен з трьох ПЗ відрізняється у встановленні та налаштуванні.

Виходячи з аналізу вразливостей мережі та моделі загроз зловмисників, яка була представлена в аналітичній частині, можна зробити висновок, що для повноцінного моніторингу мережі компанії нам потрібні дві системи виявлення вторгнень від компанії ТОВ «ТЕЛЕМАРТ» (ViPNet IDS 2000 Версії 2). Одна з них буде відповідальна за моніторинг трафіку і фільтрацію подій в локальній мережі, а інша - за моніторинг трафіку Інтернету, що надходить з мережі. Для відображення трафіку локальної мережі і трафіку з мережі Інтернет обидві IDS підключаються до комутатора і маршрутизатора відповідно через SPAN порт. На обох IDS встановлені оновлені бази Snort IDS, а також укладений договір з компанією ТОВ «ТЕЛЕМАРТ» на щомісячне їх оновлення. IDS надсилає сигнали групі реагування при виявленні інцидентів.

Кожна IDS безпосередньо підключена до системи, яка була придбана у компанії ТОВ «ТЕЛЕМАРТ» - ViPNet Threat Intelligence Analytics System (ViPNet IDS TIAS). Ця система використовується для повторного глибокого аналізу відфільтрованих інцидентів, створення карток інцидентів для унікальних ситуацій і висунення рекомендацій для персоналу, які стосуються ймовірних негайних дій з даного інциденту. Усі сервери і робочі місця, які ведуть журнали

подій, підключені до ViPNet IDS TIAS для забезпечення даними при виникненні інцидентів з використанням цих пристроїв.

Через захищене з'єднання VPN, в мережі Інтернет, система ViPNet IDS TIAS також підключена до аналогічних систем у філіях підприємства для обміну інформацією щодо інцидентів, що виникли в них і не зачепили головний центр обробки та зберігання інформації компанії.

Уся система централізованого управління має доступ через захищене з'єднання через ViPNet Coordinator HW1000, встановленому в компанії.

Після введення в експлуатацію комплексу ViPNet Office Firewall, програмна (рис.2.15) і технічна (рис.2.16) архітектура підприємства «ЯВІР ДНІПРО-1» зазнає змін у своєму вигляді.

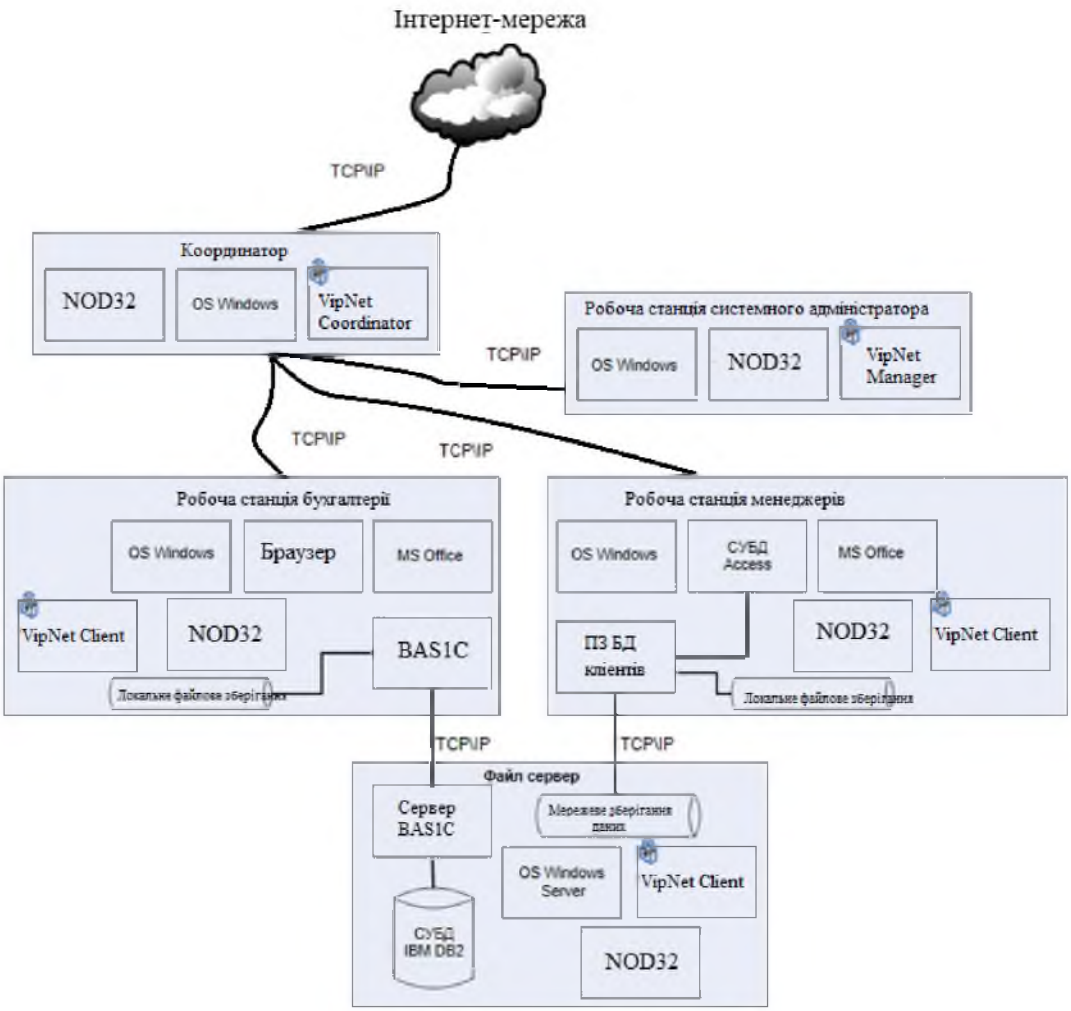


Рисунок 2.15 - Програмна архітектуру ІС «ЯВІР ДНІПРО-1» після проєктування

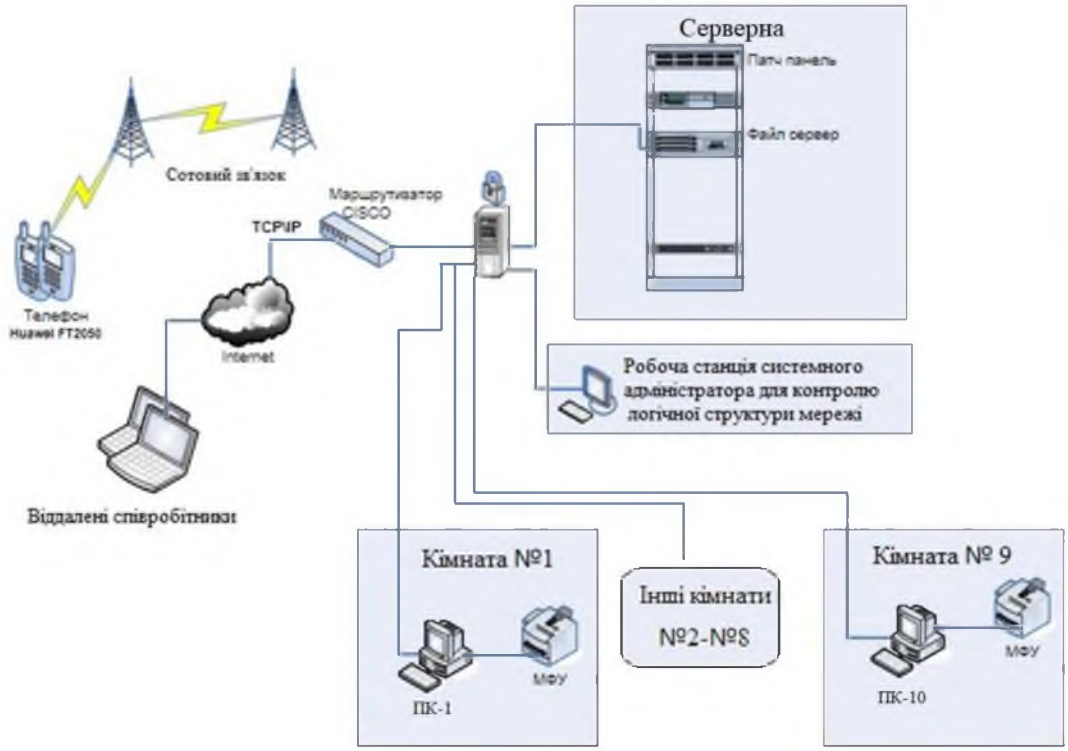


Рисунок 2.16 - Технічна архітектуру ІС «ЯВІР ДНІПРО-1» після проєктування

Цей комплекс систем моніторингу дозволяє підвищити ймовірність виявлення інцидентів, які не сталися в мережі компанії, завдяки постійного оновлення правил, що закуповуються у компанії ТОВ «ТЕЛЕМАРТ», та передчасних сповіщень про інциденти, які відбуваються з інформаційними ресурсами. Розподіл моніторингу трафіку між локальним трафіком і трафіком, що надходить в інтернет-мережі, дозволяє прискорити реакцію на інцидент завдяки зручнішому представленню інформації; оперативно визначити джерело комп'ютерної атака і вжити заходів для її припинення, тим самим знизивши критичність інциденту до мінімуму, а також зменшити навантаження на апаратуру, що знизить ймовірність відмови.

Підключення локальних систем (серверів, робочих станцій і інших), що мають журнали подій, до єдиного інтерфейсу дозволяє збільшити швидкість розслідування інцидентів, виявлення пролому в мережі підприємства і пошуку зловмисника. Оскільки програмно-апаратні комплекси ViPNet IDS TIAS, розташовані у філіях і основному центрі обробці інформації, взаємодіють між

собою, це дозволяє локалізувати інцидент і зменшити критичність проведеної атаки. Іншими словами, якщо комп'ютерна атака, виконана за допомогою знайденої уразливості, відбулася в філії підприємства, своєчасне сповіщення на апаратному рівні дозволить усунути наявний пролом мережі в інших філіях підприємства і запобігти проведенню атаки з використанням цієї уразливості.

Система ViPNet IDS TIAS, завдяки своїй самонавчальності та автоматичному створенню карток інцидентів, які потім удосконалюються через глибокий аналіз фахівцями інформаційної безпеки підприємства, дозволяє зменшити ймовірність повторення інцидентів в мережі підприємства. Готові рекомендації, видаються системою ViPNet IDS TIAS для вже відомих інцидентів, дозволяють приймати рішення щодо припинення атаки без необхідності проведення додаткового аналізу.

2.7 Тестування та моделювання атаки інтернет-мережі «ЯВІР ДНІПРО-1»

Для імітаційного моделювання була обрана атаки APT41. APT41 - це група кіберзлочинців з Китаю, яка спеціалізується на шпигунстві та атаках у галузях охорони здоров'я, телекомунікацій, технологій і відеоігор у 14 країнах.

Для перевірки ефективності виявлення атаки APT41 та прогнозування подальших дій, пов’язаних із цією атакою, необхідно підготувати 64 log-файлам, в яких, крім симптомів атаки, також будуть включені записи про дії легітимних користувачів.

Для моделювання атаки будуть використані наступні симптоми, які є частиною атаки APT41:

1. External Remote Services - цей симптом ілюструє підключення зловмисника через видалений зовнішній сервіс з можливістю закріплення усередині системи. Такими сервісами можуть бути SSH або VPN;

2. Valid Accounts - цей симптом полягає в авторизації порушника безпеки за допомогою облікових даних легітимних користувачів;

3. Command-Line Interface - це використання зловмисником інтерфейсу командного рядка для взаємодії з операційною системою;

4. Create Account - цей симптом передбачає створенням зловмисником аккаунта на цільовій системі для того, щоб забезпечити собі безперешкодний вхід в систему без необхідності повторного зламу;

5. Clear Command History - ця ознака визначається очищенням історії команд в терміналі або командному рядку;

6. Brute Force - це перебір всіляких комбінацій облікових даних при спробі підключитися до легітимного облікового запису;

7. File Deletion - це вилучення файлів комбінацій облікових даних при спробі підключитися до легітимного облікового запису;

8. System Network Configuration Discovery - цей симптом передбачає спроби зловмисника дізнатися інформацію про мережу, до якої він підключився. Це можуть бути спроби дізнатися 63 топологію мережі, з'ясувати, які мережеві інтерфейси відкриті в системі, до якої він підключився і так далі;

9. Network Service Scanning - це спроба зловмисника визначити список запущених сервісів на хості та знайти серед них уразливість для видаленого експлойту. Про наявність цього симптому може свідчити використання порушником інформаційної безпеки сканерів портів;

10. System Owner/User Discovery - ця ознака характеризується використанням порушником інформаційної безпеки стандартних засобів операційної системи, для визначення списку користувачів, які в даний момент авторизовані в системі;

11. System Network Connections Discovery це дослідження та отримання списку витікаючих підключень, що входять, усередині системи, в якій авторизований порушник ІБ;

12. Data compressed - це використання зловмисником алгоритмів компресії для стиснення необхідних файлів та даних з метою подальшої передачі через скомпрометовану мережу на свій ресурс. Стискування потрібне для зниження навантаження на мережу під час передачі, що дозволяє зменшити ризик виявлення.

Ознаки симптомів External Remote Services та Valid Accounts знаходяться у log-файлі auth.log. Інформацію щодо симптомів Command-line Interface, Create Accounts, File Deletion, Data Compressed, System Network Connections Discovery, System Owner/User Discovery, System Network Configuration Discovery можна знайти у файлах .bash_history користувачів і файлі .bash_history адміністратора. У випадку відсутності таких файлів або установці того факту, що вони були очищені, можна стверджувати про наявність ознаки APT-атаки, такої як Clear Command History. Інформацію щодо ознаки Brute Force можна знайти як у файлі auth.log так і у файлі secure.log.

Вміст log-файлу представлений в додатку Д.

Саме моделювання атаки відбувалося в операційній системі Debian GNU/Linux 9 (stretch) з версією ядра 4.9 GHz. Ланцюжок дій, здійснюваний для моделювання атаки, представлений у Додатку Е. Після моделювання атаки там дій легітимних користувачів операційної системи, ми запустимо впроваджену систему ViPNet IDS для аналізу log-файлів і пошуку в них ознак змодельованої атаки. Рис.2.17 - 2.20 ілюструють результати аналізу log-файлів системою.

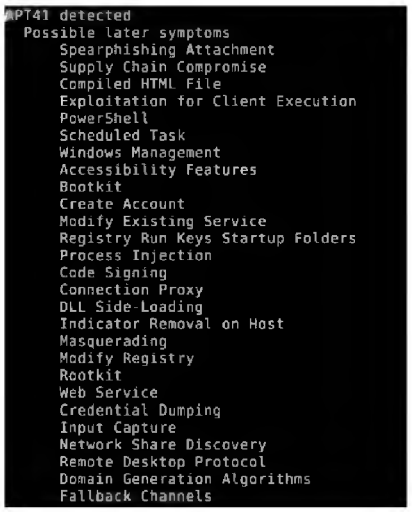


Рисунок 2.17 - Повідомлення про виявлену атаку APT41 і прогнозування подальших дій зловмисника

```
APT32 detected
  Possible later symptoms
      Driver-by Compromise
      Spearphishing Attachment
      Spearphishing Link
      Exploitation for Client Execution
      Mshta
      PowerShell
      Regsvr32
      Scheduled Task
      Scripting
      Service Execution
      Signed Script Proxy Execution
      User Execution
      Windows Management
      Hidden Files and Directories
      Modify Existing Service
      New Service
      Office Application Startup
      Registry Run Keys Startup Folders
      Exploitation for Privilege Escalation
      Binary Padding
      Credential Dumping
      Pass the Hash
      Pass the Ticket
      Remote File Copy
      Data Encrypted
      Commonly Used Port
      Custom Command and Control Protocol
```

Рисунок 2.18 - Повідомлення про виявлену атаку APT32 і прогнозування подальших дій зловмисника

Як можна помітити, результати роботи модуля прогнозування ілюструють ознаки APT41 і APT32, які можуть з'явитися при подальшому розвитку поточної атаки. Нижче представлені скріншоти результатів побудови вектору вже виявлених ознак розвитку атаки.

```
One sub graph
  One symptom
      Time: 2020/5/20/0:43:0
      Category: files_and_directory_discovery
      Information: 291.235.112.122
  One symptom
      Time: 0/0/0/0:0:0
      Category: network_service_scanning
      Information: 291.235.112.122
      Information: 78.12.281.112
  One symptom
      Time: 2019/12/5/01:02:35
      Category: brute_force
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:38
      Category: external_remote_service
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:32
      Category: valid_accounts
      Information: 291.235.112.122
      Information: Denis
  One symptom
      Time: 2019/12/5/01:15:32
      Category: command_line_interface
      Information: Denis
      Information: bash
  One symptom
      Time: 0/0/0/0:0:0
      Category: system_owner_user_discovery
      Information: Denis
      Information: who
      Information: args:
  One symptom
      Time: 0/0/0/0:0:0
      Category: system_network_connections_discovery
      Information: Denis
      Information: lsof
      Information: args: -U | head -5
```

Рисунок 2.19 - Перша частина графа виявлених ознак атаки

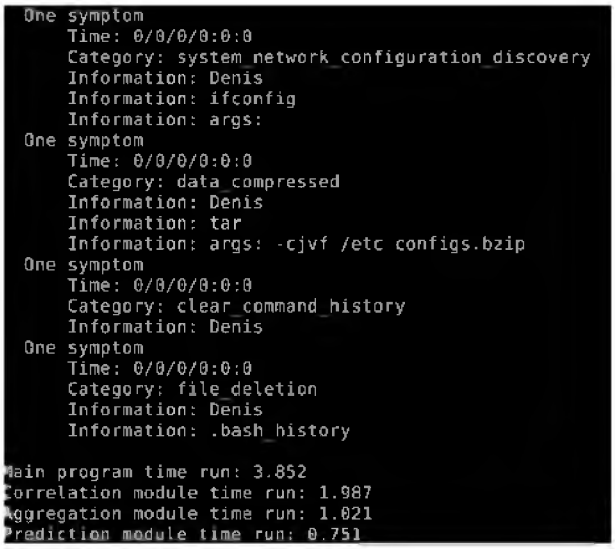


Рисунок 2.20 - Друга частина графа виявлених ознак атаки

Як можна бачити на рисунках вище, система Snort IDS виявила всі змодельовані автором симптоми і побудувала на їх основі вектор атаки. Слід звернути увагу, що впроваджена система моніторингу та управління подіями ІБ виявляє атаку при виявленні взаємозв'язку між певною кількістю подій ІБ. Ця кількість залежить від пріоритету для кожної з подій. Наприклад, якщо двох ознак встановлений високий пріоритет, то при виявленні взаємозв'язку навіть між ними буде сформовано повідомлення про цільову атаку. З іншого боку, якщо у подій встановлений нижчий пріоритет, то для формування повідомлення про можливий інцидент інформаційної безпеки потрібно буде знайти взаємозв'язок між багатьма подіями.

Для систему ViPNet IDS всі ці події рівноцінні, і весь процес пошуку взаємозв'язків між ними лягає на плечі адміністратора інформаційної безпеки.

2.8 Оцінка ефективності тестування інтернет-мережі «ЯВІР ДНІПРО-1»

Перед формулюванням остаточних висновків проєкту, важливо оцінити ефективність впроваджуваної системи Snort IDS. Це дозволить зробити більш повні та фактами підкріплені висновки. Як вже було сказано вище, система успішно виявила всі змодельовані симптоми та ефективно сформувала

повідомлення об наявність атаки APT41. Також було створені повідомлення щодо подальшого розвитку цієї та інших атак.

Програма відпрацювала за 3.852 секунд.

Графічно, час роботи кожного з модулів представлений на рис. 2.21

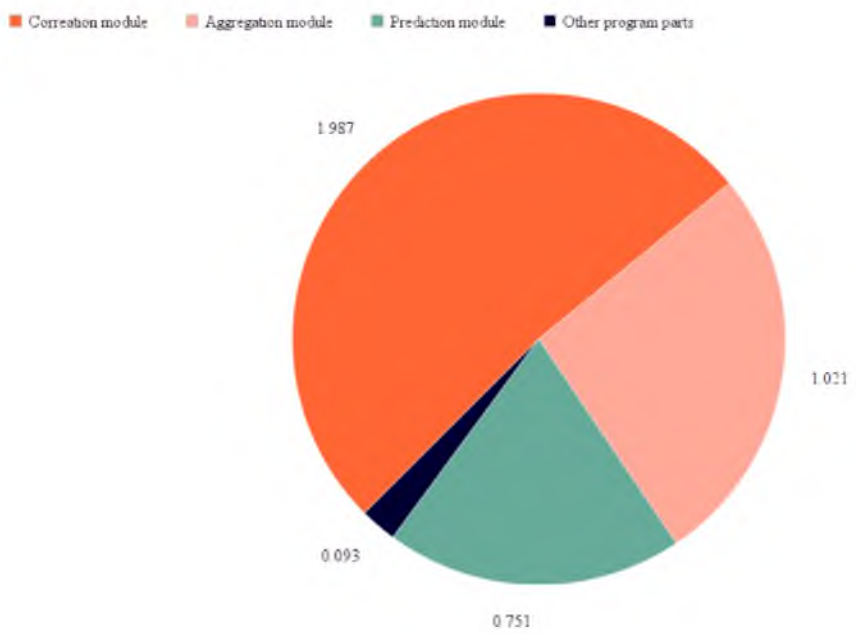


Рисунок 2.21 - Діаграма часу виконання модулів системи

На діаграмі видно, що час роботи модуля кореляції майже вдвічі більший, ніж час роботи модуля агрегації і майже втричі перевищує роботу модуля прогнозування. Важливо відзначити, що при збільшенні розміру графа виявлених подій інформаційної безпеки розрив у часі між модулем кореляції і модулями агрегації і прогнозування збільшуватиметься через алгоритм пошуку взаємозв'язків між подіями інформаційної безпеки.

2.9 Висновок

Програмне забезпечення ViPNet Client призначене для використання в мережах ViPNet, керованих за допомогою ПЗ ViPNet Administrator і ПЗ ViPNet Network Manager. ViPNet Client виконує функції VPN-клієнта в мережі ViPNet і забезпечує захист комп'ютера від несанкціонованого доступу при роботі в локальних або глобальних мережах. Програмне забезпечення ViPNet Client може

бути встановлене для захисту трафіку на будь-якому комп'ютері з ОС Windows, будь то стаціонарний, видалений, мобільний комп'ютер або сервер.

Впровадження програмного комплексу ViPNet Office охопить всі структурні підрозділи підприємства, оскільки програма надає повний контроль над усією локальною мережею, розгорнутою на підприємстві. Це включає в себе:

1. технологія побудови мереж VPN ViPNet;
2. система захисту інформації ViPNet;
3. адміністрування системи захисту інформації ViPNet;
4. засвідчуючий центр ViPNet;
5. програмний комплекс ViPNet Client;
6. комплексний захист конфіденційної інформації;
7. практикум по використанню програмного забезпечення ПЗ ViPNet.

Можливості:

- динамічна і статична трансляція мережевих адрес NAT;
- підтримка протоколу FTP;
- веб-фільтрація;
- автозаповнення правил трансляції мережевих адрес NAT;
- антиспуфінг;
- фільтрація локальних і транзитних IP-пакетів по адресах одержувача і відправника;
- фільтрація широкомовних IP-пакетів по адресах відправника;
- робота мережевих фільтрів за розкладом;
- застосування мережевих фільтрів в заданому порядку;
- система виявлення атак IDS;
- журнал IP-пакетів з урахуванням пари адрес і трансляції мережевих адрес NAT;
- створення декількох конфігурацій і швидке перемикання.

Головні переваги програми:

- підтримка необмеженої кількості мережевих адаптерів;
- підтримка різних способів підключення до мережі;

- вбудований контроль додатків для виявлення і обмеження мережевої активності програм «шпигунів»;

- обов'язкове введення пароля програми при вході в операційну систему;

- використання drag-and-drop в інтерфейсі програми для переміщення фільтрів;

- можливість швидкого блокування мережевого трафіку і "робочого столу" комп'ютера;

- підтримка протоколу SIP для автоматичного відкриття портів, необхідних для роботи SIP-клієнтів, що забезпечують роботу VoIP-телефонії.

Використання ViPNet Office Firewall в «ЯВІР ДНІПРО-1»:

- Захист локальної мережі від атак з Інтернет - ViPNet Office Firewall дозволяє захистити локальну мережу від зловмисників, які не лише сканують Ваш сервер-шлюз, а й намагаються проникнути в Вашу локальну мережу. Для цього досить встановити зовнішній мережевий адаптер сервера (підключений до мережі Інтернет) в режим "Бумеранг" ("Stealth").

- Управління доступом до Інтернет-ресурсів з локальної мережі: Окрім захисту від атак з Інтернету, ViPNet Office Firewall дозволяє заборонити роботу в Інтернеті певним комп'ютерам локальної мережі, користувачам яких такий доступ для службових потреб не потрібен, або дозволити окремим комп'ютерам працювати в мережі тільки з певними сервісами, наприклад, поштовими серверами. В цьому випадку достатньо задати фільтри для IP-адрес комп'ютерів або діапазонів адрес і вказати, що трафік з цих адрес має бути заблокований або дозволений.

- Організація віртуальних мереж: ViPNet Office Firewall підтримує необмежену кількість мережевих адаптерів, і для кожного мережевого адаптера можна задати свій режим і свої фільтри. Завдяки цьому можна розділити дві або три локальні мережі, наприклад, так, щоб з першої мережі в другу доступ був відкритий, а навпаки - ні (чи тільки певним комп'ютерам був би дозволений доступ). Також є можливість організації так званої «демілітаризованої зони» (ДМЗ), в якій розмістити сервера, відкриті для доступу з Інтернету. При цьому

вихідний трафік з ДМЗ в локальні мережі, підключені до інших внутрішніх адаптерів, можна повністю заблокувати.

Великий рівень фільтрації трафіку надає можливість захисту голосового і відеозв'язку, дозволяє отримувати доступ до корпоративних інформаційних систем незалежно від геолокації користувача, а при цьому захищає канал і не впливає на роботу інших програм на ПК користувача. Передача політики безпеки, ключів шифрування і оновлень відбувається через надійний і захищений канал.

ViPNet встановлюється на робочі станції і сервера для забезпечення мандатного і дискреційного розмежування доступу користувачів до критично важливої інформації та підключених пристроїв. Реалізовані розмежувальні політики (між користувачем і об'єктами) і розділові політики (між користувачами), що ґрунтуються на автоматичній розмітці файлів, дозволяють впроваджувати механізми захисту від зовнішніх та внутрішніх загроз.

Основою захисних механізмів продукту є можливість застосування розмежувальних політик до файлів (як до вже існуючих, так і до новостворених), реєстру і процесів операційної системи, а також до підключених по мережі друкарських пристроїв.

Такий підхід дозволяє захиститися від:

- випадкових і зловмисних дій внутрішніх користувачів;
- атак підвищеного рівня привілеїв;
- впровадження та виконання шкідливих програм, як зовнішніх, так і від внутрішніх загроз;
- неправомірного використання підключених пристроїв.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою дипломної роботи є аналіз та підвищення рівня захищеності інтернет-мережі «ЯВІР ДНІПРО-1». Витоки/втрати інформації, котра є критично важливою для кожного підприємства, можуть призвести до матеріальних збитків.

Метою економічного розділу є визначення економічної доцільності впровадження запропонованих мір зі зниження ризиків.

Задачами економічного розділу є встановлення:

- витрат на придбання і налагодження мір зі зниження ризиків в установі;
- річних експлуатаційних витрат, необхідних для підтримання та ефективного функціонування придбаних;
- оцінка економічної ефективності.

3.1 Розрахунок (фіксованих) капітальних та поточних витрат

Капітальні інвестиції - це кошти, спрямовані для створення і придбання основних фондів і нематеріальних активів, які підлягають амортизації.

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{дм} + К_{навч} + К_{н}\text{ , грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження та залучення для цього зовнішніх консультантів, грн.

$К_{зпз}$ - вартість закупівлі ліцензійного основного та додаткового ПЗ, грн.

$К_{рп}$ - вартість розробки програми підвищення обізнаності, грн.

$К_{аз}$ - вартість закупівлі апаратного забезпечення, грн.

$К_{дм}$ - вартість допоміжних матеріалів, грн.

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, грн. Дані витрати не враховуються під час розрахунків, оскільки фахівці не проходили платного навчання.

$К_н$ - витрати на встановлення та налагодження системи по захищеності інтернет-мереж, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження комплексу програмних засовів: ViPNet Office Firewall, Threat Intelligence, Snort IDS, та програмно-апаратних засовів захисту інформації: IDS 2000 Q2, ViPNet Coordinator HW1000.

3.1.1 Визначення трудомісткості розробки підвищення захищеності інтернет-мережі.

Трудомісткість розробки політики підвищення рівня захищеності інтернет-мережі визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційною безпекою):

$$Т= t_{тз} + t_в + t_{вз} + t_{озб} + t_{опр} + t_д, \quad \text{годин.} \qquad (3.2)$$

де $t_{тз}$ - тривалість складання технічного завдання на розробку;

$t_в$ - тривалість розробки концепції безпеки інформації у організації;

$t_{вз}$ - тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ - тривалість вибору основних рішень з забезпечення безпеки мережі;

$t_{опр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ - тривалість документального оформлення на ПК.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій складається з наступних величин: $t_{тз}$ = 20 годин, $t_в$ = 20 годин, $t_{вз}$=15 годин, $t_{озб}$=8 годин, $t_{опр}$=40 годин, $t_д$=6 годин.

Згідно формули 3.2:

$$Т = 20 + 20 + 15 + 8 + 40 + 6 = 109 \text{ годин.}$$

3.1.2 Розрахунок витрат на створення політики підвищення захищеності інтернет-мереж.

Витрати на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$.

$$З_{зп} = Т \cdot З_{пр} = 109 \cdot 240 = 26160 \text{ грн.} \qquad (3.3)$$

$З_{пр}$ - середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, 240 грн/годину.

Вартість машинного часу для розробки політики підвищення захищеності інтернет-мережі на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_д, \quad \text{грн.} \tag{3.4}$$

де $t_{опр}$ - трудомісткість налагодження програми на ПК, год;

$С_{мч}$ - вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_д \cdot C_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн.} \tag{3.5}$$

де Р - встановлена потужність ПК, Р = 0,8 кВт ;

$С_е$ - тариф на електричну енергію, $С_е$ = 2,64 грн/кВт-година;

$Ф_{зал}$ - залишкова вартість ПК на поточній рік, грн;

$Н_а$ - річна норма амортизації на ПК, частка одиниці;

$Н_{апз}$ - річна норма амортизації на ліцензійне програмне забезпечення, часта одиниці;

$К_{лпз}$ - вартість ліцензійного програмного забезпечення, грн;

$F_р$ - річний фонд робочого часу (1920).

$$C_{мч} = 0,8 \cdot 6 \cdot 2,64 + \frac{5500 \cdot 0,6}{1920} + \frac{3500 \cdot 0,2}{1920} = 14,76 \text{ грн.}$$

$$З_{мч} = 40 \cdot 14,76 + 6 = 596,4 \text{ грн.}$$

3.1.3 Розрахунок капітальних витрат

Відповідно до розроблених рекомендації щодо удосконалення та захисту системи інтернет-мережі «ЯВІР ДНІПРО-1», необхідно придбати програмний пакет ViPNet Office Firewall, в який входить підтримка та керування програмно-апаратними комплексами:

1. IDS 2000 Q2, на базі сервера AquaServer T50 D14, для виявлення атак.

2. ViPNet Coordinator HW1000, на базі сервера AquaServer T40 S44 для аналізу шкідливих кодів та виступати в якості VPN-шлюза.

Також необхідні додаткові витрати на оновлення та підтримку правил Snort IDS, які допоможуть скоротити час роботи програмно-апаратного комплексу.

Вартість затрат:

1. Апаратне забезпечення
   1.1. Сервер AquaServer T50 D14 - 81421 грн.
   1.2. Сервера AquaServer T40 S44 – 48562 грн.
2. Програмне забезпечення
   2.1. ViPNet Office Firewall - 28000 грн на 2 роки
   2.2. Snort IDS – 24000 грн на 2 роки.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають (3.1):

1. Вартість впровадження та залучення зовнішніх консультантів Кпр=0 грн. Сторонні організації не залучалися, тому цей коефіцієнт не враховується при розрахунках.

2. Вартість закупівлі ліцензійного основного та додаткового ПЗ:

$$К_{зпз} = 28000+24000 = 52000 \text{ грн.}$$

3. Вартість розробки програми підвищення обізнаності:

$$К_{рп} = З_{зп} + З_{мч} = 26160 + 596,4 = 26756,4 \text{ грн.} \quad (3.6)$$

4. Вартість закупівлі апаратного забезпечення:

$$К_{аз} = 81421 + 48562 = 129983 \text{ грн.}$$

5. Вартість допоміжних матеріалів $К_{дм} = 0$ грн.

6. Витрати на навчання технічних фахівців і обслуговуючого персоналу $К_{навч} = 0$ грн, ці витрати не враховуються під час розрахунків, оскільки фахівці не проходили платного навчання.

7. Витрати на встановлення та налагодження системи по захищеності інтернет-мережі Кн = 0 грн. У штаті є 2 працівника IT-відділу, які цим займаються в робочий час.

$$К = 52000 + 26756,4 + 129983 = 208739,4 \text{ грн.}$$

Таким чином, капітальні витрати на розробку та впровадження вимог складають 208739,4 грн.

3.1.4 Розрахунок поточних витрат

Річні поточні витрати на підвищення рівня захищеності інтернет-мережі:

$$C = C_в + C_к + C_{ак}, \quad грн. \tag{3.7}$$

де $C_в$ - вартість відновлення й модернізації системи ($C_в = 0$);

$C_к$ - витрати на керування системою в цілому;

$C_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($C_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки складають:

$$C_к = C_н + C_а + C_з + C_{єсв} + C_{ел} + C_{тос} + C_{ін}, \text{ грн.} \tag{3.8}$$

Витрати на навчання адміністративного персоналу $C_н = 5000$ грн.

Річні амортизаційні відрахування на оновлення та підтримку програмного пакет ViPNet Office Firewall та правил Snort IDS з корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$$C_а = (28000 + 24000) / 2 = 26000 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, складає:

$$C_з = З_{осн} + З_{дод}, \text{ грн.} \tag{3.9}$$

У даному випадку в штаті «ЯВІР ДНІПРО-1» вже є системний адміністратор та спеціаліст з питання кібербезпеки $C_з = 0$ грн. і $C_{єсв} = 0$ грн.

Вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року ($C_{ел}$), визначається за формулою:

$$C_{ел} = P_н \cdot F_р \cdot C_е, \quad грн. \tag{3.10}$$

де $P_н$ - встановлена потужність додаткової апаратури підвищення рівня захищеності інтернет-мереж, $P_н = 1,4$ кВт;

Вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$С_{ел} = 1,4 \cdot 1920 \cdot 2,64 = 7096,32 \text{ грн.}$$

Витрати на технічне та організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% :

$$С_{тос} = К \cdot 2\% = 208739,4 \cdot 0,02 = 4174,79 \text{ грн.} \quad (3.11)$$

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 5000 + 26000 + 7096,32 + 4174,79 = 42271,11 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 42271,11 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ - час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_{о1}$ - заробітна плата обслуговуючого персоналу (системного адміністраторів та), 18000 грн./міс.;

$З_{о2}$ - заробітна плата обслуговуючого персоналу (спеціаліста з питання кібербезпеки), 22000 грн./міс.;

$З_с$ - заробітна плата співробітників, 21000 грн./міс.;

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 8 осіб.;

О - обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1200 тис. грн. у рік;

$П_{зч}$ - вартість заміни встаткування або запасних частин, 0 грн;

I - число атакованих сегментів корпоративної мережі, 1;

N - середнє число атак на рік, 60.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \qquad (3.12)$$

де $П_п$ - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п = \frac{21000 \cdot 8}{176} \cdot 4 = 3818{,}18 \quad \text{грн.} \qquad (3.13)$$

де F - місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \qquad (3.14)$$

де $П_{ви}$ - витрати на повторне уведення інформації, грн.;

$П_{пв}$ - витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} = \frac{21000 \cdot 8}{176} \cdot 6 = 5727,27 \text{ грн.} \quad (3.15)$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в = \frac{18000 + 22000}{176} \cdot 2 = 454,55 \text{ грн.} \quad (3.16)$$

$$П_в = 5727,27 + 454,55 = 6181,82 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи з середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \quad (3.17)$$

$$V = \frac{1200000}{2080} \cdot (4 + 2 + 6) = 6923,08 \text{ грн.}$$

де $F_г$ - річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 3818,18 + 6181,82 + 6923,08 = 16923,08 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = 60 \cdot 1 \cdot 16923,08 = 1015384,8 \text{ грн.} \quad (3.18)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = B \cdot R - C_к, \text{ грн.} \quad (3.19)$$

де B - загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R - вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 1015384,8 \cdot 0,35 - 42271,11 = 313113,57 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності захищеності інтернет-мережі

Коефіцієнт повернення інвестицій ROSI визначає, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій у впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці} \quad (3.20)$$

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{313113,57}{208739,4} = 1,5, \quad \text{частки одиниці,}$$

Проєкт вважається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.21)$$

де $N_{деп}$ - річна депозитна ставка, (18 %);

$N_{інф}$ - річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,5 > (18 - 11)/100$$

$$0,65 > 0,07.$$

Термін окупності капітальних інвестицій T_o вказує на те, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{1,5} = 0,67 \text{ років} \quad (3.22)$$

3.4 Висновок

В результаті проведення економічних розрахунків для оцінки вартості та рентабельності впровадження щодо підвищення рівня захищеності інтернет-мережі «ЯВІР ДНІПРО-1» виявлено його економічну доцільність. Капітальні та експлуатаційні витрати у цьому випадку менше можливого відверненого збитку. Капітальні витрати становлять 208739,4 грн., експлуатаційні 42271,11 грн. Величина річного економічного ефекту складає 313113,57 грн. Коефіцієнт повернення інвестицій ROSI складає 1,5 одиниць, а термін окупності капітальних інвестицій становить 7 місяців. Впровадження цих заходів стає необхідною умовою для подальшого розвитку діяльності підприємства.

ВИСНОВКИ

У ході виконання роботи виконано аналіз існуючої інтернет-мережі підприємства. Було проведено дослідження можливих варіантів використання засобів захисту інформації у комп'ютерній мережі «ЯВІР ДНІПРО-1». На підставі проведеного дослідження визначені найбільш ефективні засобі захисту, механізм їх роботи та запропоновані заходи до покращення захисту інтернет-мережі.

Практична цінність роботи полягає в підвищенні рівня захищеності інтернет-мережі шляхом програмних, апаратних і організаційних заходів підприємства «ЯВІР ДНІПРО-1» шляхом впровадження засобів захисту інформації циркулюючої у мережі, а також удосконалення існуючої системи інформаційної безпеки мережі.

У економічному розділі був здійснений розрахунок економічного ефекту від впровадження та налагодження розроблених засобів захищеності інтернет-мережі «ЯВІР ДНІПРО-1», спрямованих на зменшення збитків від атак на мережу. На підставі отриманих результатів, коефіцієнт повернення інвестицій ROSI складає 1,5 грн./грн., а термін окупності капітальних інвестицій складає до 7 місяців. Було доведено, що впровадження запропонованих удосконалень у систему захисту комп'ютерній мережі «ЯВІР ДНІПРО-1» є економічно ефективним рішенням.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994).

2 Закон України “Про захист персональних даних” (2010).

3 Домарьов В.В. Безпека інформаційних технологій. Методологія створення систем захисту. - К.: ТОВ ТІД ДС ISBN: 966-7992-02-0, 2001. -688 с.

5 Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков - К.: Видавнича група BHV, 2009. - 608 с.

6 Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: Монографія. - Запоріжжя: ГУ “ЗІДМУ”, 2003 - 250 с.

7 О. М. Черкун Сучасні технології комп’ютерної безпеки: колективна монографія. - Рівне: МЕГУ, 2012. - 90 с.

8 Одеський національний економічний університет. Інформатика та інформаційні технології: студентська наукова конференція, 20 квітня - 15 травня 2021 року 67с.

9 Безпека банківської діяльності: монографія / Н. Ф. Казакова, В. І. Панфілов, Л. М. Скачек, О. О. Скопа, В. О. Хорошко. - К.: ПВП «Задруга», 2013. - 282 с.

10 О. В. Орлик. Економічна безпека в умовах глобалізації світової економіки: Дніпропетровськ: «ФОП Дробязко С.І.», 2014. - Т. 2. - 268с.

11 О. В. Орлик. Modern problems of regional development: Collection of scientific articles. - 2014. - Vol. 2. - P. 190-194.

12 Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. - 2013. - № 15(204). - Ч. 1. - С. 59-62.

13 Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич,. - К.: Кондор, 2005. -382 с.

14 Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. 414 с.- К. : ДУІКТ, 2006. -закл.] / В.М. Богуш, А. М. Кудін.

15 Менаске Д. Продуктивність Web-служб. Аналіз, оцінка та планування / Менаске Д., 480 с.: ДіаСофтЮп", 2012. Віргіліо А.; пров. з англ.

16 Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. - Х. : Вид. ХНЕУ, 2013. - 476 с.

17 Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. 2007. - 209 с. - К.: ПоліграфКонсалтинг. -Терейковський.

18 Щеглов А. Ю. Захист комп'ютерної інформації від несанкціонованого доступу/А. Ю. Щеглов. - К.: Наука та техніка, 2012. - 384 с.

19 Гундар К. Ю. Захист інформації у комп'ютерних системах / К. Ю. Гундар, А. Ю. Гундар, Д. А. Янішевський. – К.: «Корнійчук», С. 2002. -152.

20 NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications//National Institute of Standards and Technology Special Publication 800-22rev1a, 2023, - 131 p.

21 Internet для користувача: [навч. посіб.] / В. М. Антоненко, Б. Д. Пацай, Л. О. Терейковська, І. А. Терейковський; Держ. податк. адмін. України, Нац. ун-т держ. податк. служби України. - Ірпінь: НУ ДПС України, 2010. - 244 с.: іл., табл. - Бібліогр.: с. 227. - Предм. покажч.: с. 242-244.

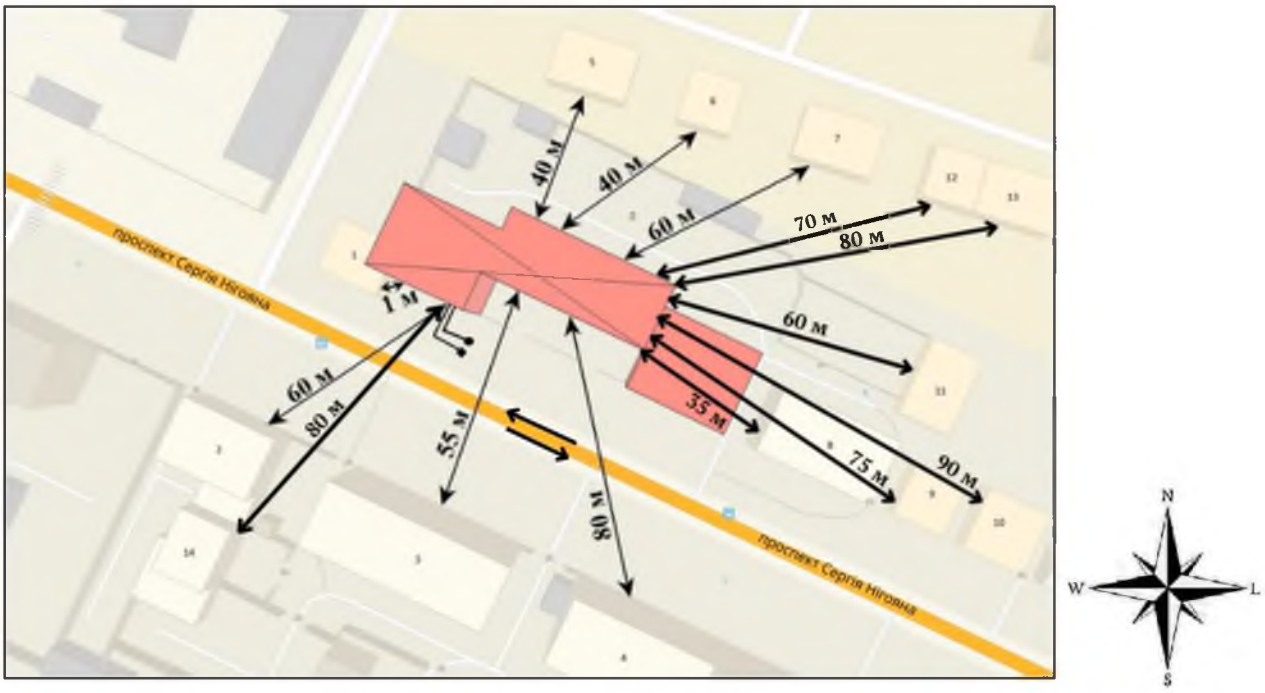
22 Комп'ютерне моделювання інформаційно-аналітичних систем / О. Г. Додонов, О. В. Коваль, Л. С. Глоба, Ю. Д. Бойко; НАН України, Ін-т проблем реєстрації інформації. - Київ: ІПРІ НАН України, 2017. - 238 с.: іл. - Бібліогр.: с. 225-238.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	35	
6	А4	Спеціальна частина	47	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	4	
15	А4	Додаток Е	1	
16	А4	Додаток Є	1	
17	А4	Додаток Ж	1	
18	А4	Додаток З	1	

ДОДАТОК Б. Розташування «ЯВІР ДНІПРО-1»

СИТУАЦІЙНИЙ ПЛАН
МАСШТАБ 1:500



Умовні позначення ситуаційного плану:

1 — будівля

P — місце парковки

— будівля ОЦД

— напрямок руху транспорту

— дитячий майданчик

— зупинка

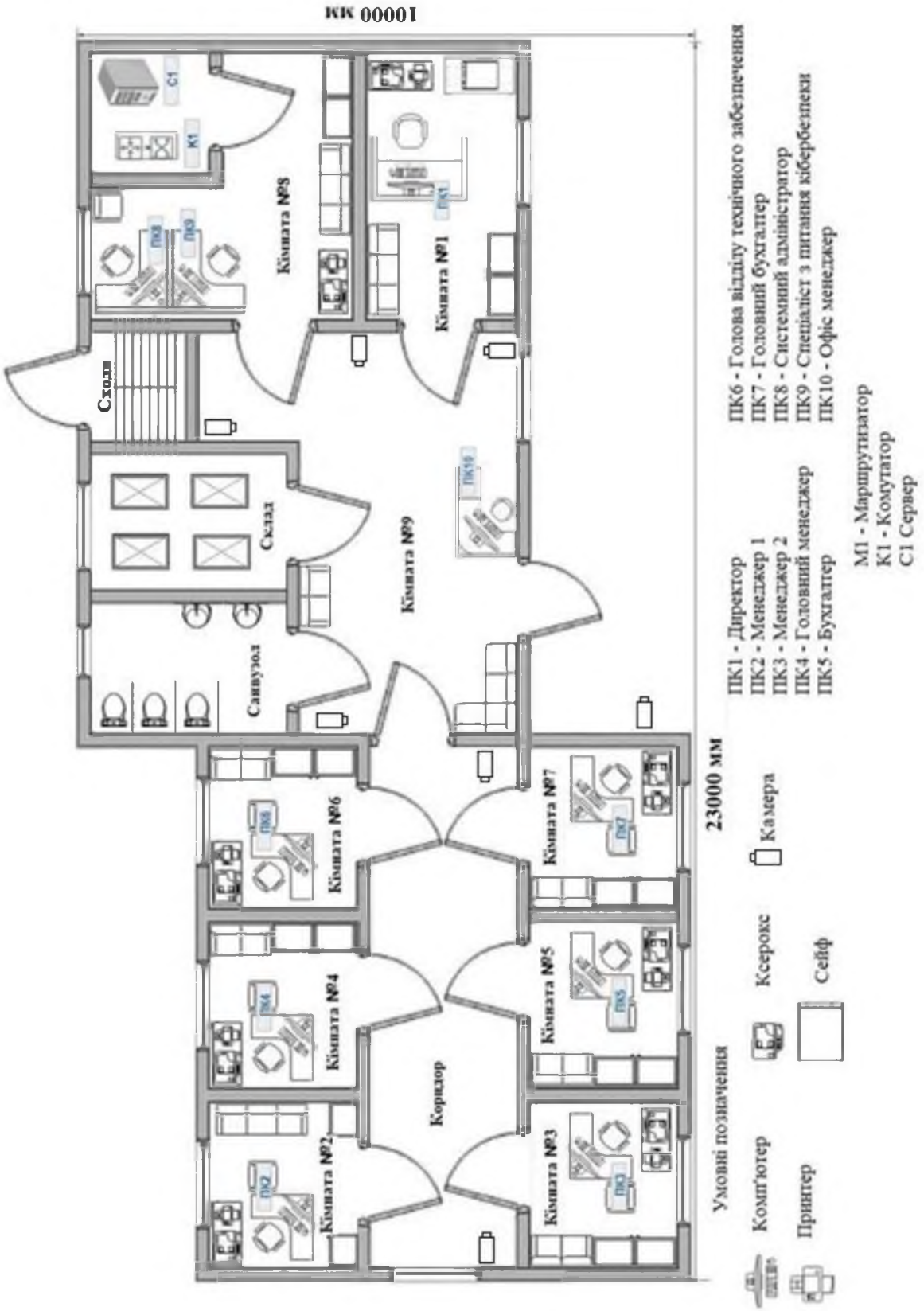
— паркан з каліткою

— контрольована зона ОЦД

— система каналізації

— система водопостачання

ДОДАТОК В. Розміщення інформаційної системи «ЯВІР ДНІПРО-1»



ДОДАТОК Г. Сертифікат відповідності

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ
ДЕРЖАВНА СИСТЕМА СЕРТИФІКАЦІЇ УкрСЕПРО

Серія ВІ

СЕРТИФІКАТ ВІДПОВІДНОСТІ

Зареєстровано в Реєстрі за № UA1.066.0037979-16
Зарегистрирован в Реестре

Термін дії з 26 жовтня 2010 **до** 25 жовтня 2027
Срок действия с

Продукція виріб "Програмний комплекс "ViPNet Office Firewall" 8539
Продукция код УКТ ЗЕД, ТН ЗЕД

код ДКПП, ОКП

Відповідає вимогам
Соответствует требованиям ДСТУ 28147:2009, ДСТУ 9041:2010

Виробник продукції відкрите акціонерне товариство "ІнфоТеКЗС"
Изготовитель продукции

Сертифікат видано Товариство з обмеженою відповідальністю "ТЕЛЕМАРТ"
Сертификат выдан

Додаткова інформація Продукція, яка виготовляється серійно та ввозиться в Україну з 26.10.2010 р. до 25.10.2025 р., з урахуванням гарантійного терміну зберігання, технічний нагляд один раз на рік.
Дополнительная информация Добровільна сертифікація

Сертифікат видано органом з сертифікації ОС 'Міжнародні стандарти і системи', м. Харків, вул. Культури, 26, оф. 13, тел. (057) 705-27-16 свідоцтво про призначення № UA.P.066 від 11.03.2013 р., свідоцтво про уповноваження № UA.PN.066 від 11.03.2013 р.
Сертификат выдан органом по сертификации

На підставі Протоколу сертифікаційних випробувань № 2016.02.10.26.16 від 26.10.2016 р., виданого ВЛ ТОВ 'АКАДЕМТЕСТ' , 61023, м. Харків, вул. Весніна, 5, атестат акредитації № 2Н1045 від 20.12.2012 р. до 19.12.2017 р.
На основании

№ 641847

Керівник органу з сертифікації А.М. Сергейчук
Руководитель органа по сертификации підпис ініціали, прізвище

М.П.

Чинність сертифіката відповідності можна перевірити в Реєстрі системи УкрСЕПРО за тел. (044) 528-54-35

ДОДАТОК Д. Вміст log-файлу атаки

.bash_history:
ls
cd config_files/
nano corr.json
atom .
cd ..
rm corr.json
cd ..
clear
cd ..
nano co
kill %1
clear
ls
who
lsof -U | head 5
sudo -s
su
ifconfig ls /etc
tar -cjvf /etc configs.bzip
cd /
find . -name "*.log"
cd /usr/bin
ls
cd /
cd /var/log
iptables.log

PCworkstation kernel: [7671.376452] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=50 ID=25852 PROTO=TCP SPT=51302 DPT=1723 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376525] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=54 ID=16457 PROTO=TCP SPT=51302 DPT=8080 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376552] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 86 Продолжение
приложения В LEN=44 TOS=0x00 PREC=0x00 TTL=41 ID=52271 PROTO=TCP SPT=51302 DPT=199
WINDOW=1024 RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.376577] Iptables: SYN packet
detectedIN=enp2s0 OUT= MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4
LEN=44 TOS=0x00 PREC=0x00 TTL=57 ID=29935 PROTO=TCP SPT=51302 DPT=111 WINDOW=1024
RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.376602] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=52 ID=58255 PROTO=TCP SPT=51302 DPT=21 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376646] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=41 ID=65329 PROTO=TCP SPT=51302 DPT=256 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376671] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=42 ID=5883 PROTO=TCP SPT=51302 DPT=993 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376696] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=57 ID=42372 PROTO=TCP SPT=51302 DPT=113 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376725] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=44 ID=13517 PROTO=TCP SPT=51302 DPT=53 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.376757] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=49 ID=32045 PROTO=TCP SPT=51302 DPT=5900 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.380303] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00

Продовження додатку Д.

PREC=0x00 TTL=40 ID=14615 PROTO=TCP SPT=51302 DPT=443 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.380342] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=51 ID=43253 PROTO=TCP SPT=51302 DPT=143 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.380367] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=52 ID=3483 PROTO=TCP SPT=51302 DPT=8888 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.380435] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=56 ID=30623 PROTO=TCP SPT=51302 DPT=445 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.381060] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 87 Продолжение
приложения В LEN=44 TOS=0x00 PREC=0x00 TTL=53 ID=10080 PROTO=TCP SPT=51302 DPT=587
WINDOW=1024 RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.381187] Iptables: SYN packet
detectedIN=enp2s0 OUT= MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4
LEN=44 TOS=0x00 PREC=0x00 TTL=53 ID=29543 PROTO=TCP SPT=51302 DPT=1720 WINDOW=1024
RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.381860] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=38 ID=14185 PROTO=TCP SPT=51302 DPT=554 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.381967] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=57 ID=53754 PROTO=TCP SPT=51302 DPT=139 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.382587] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=39 ID=32976 PROTO=TCP SPT=51302 DPT=22 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.382728] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=49 ID=46270 PROTO=TCP SPT=51302 DPT=25 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.383406] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=45 ID=43082 PROTO=TCP SPT=51302 DPT=3389 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.383509] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=50 ID=8343 PROTO=TCP SPT=51302 DPT=1025 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.384151] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=37 ID=2067 PROTO=TCP SPT=51302 DPT=3306 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.384177] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=53 ID=31929 PROTO=TCP SPT=51302 DPT=110 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.384205] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=41 ID=62110 PROTO=TCP SPT=51302 DPT=80 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.384234] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=46 ID=11269 PROTO=TCP SPT=51302 DPT=23 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.384359] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 88 Продолжение
приложения В LEN=44 TOS=0x00 PREC=0x00 TTL=38 ID=48831 PROTO=TCP SPT=51302 DPT=995
WINDOW=1024 RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.385046] Iptables: SYN packet
detectedIN=enp2s0 OUT= MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4
LEN=44 TOS=0x00 PREC=0x00 TTL=51 ID=54463 PROTO=TCP SPT=51302 DPT=135 WINDOW=1024
RES=0x00 SYN URGP=0 PCworkstation kernel: [7671.385145] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=55 ID=15339 PROTO=TCP SPT=51302 DPT=1057 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.385697] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00
PREC=0x00 TTL=40 ID=17559 PROTO=TCP SPT=51302 DPT=7100 WINDOW=1024 RES=0x00 SYN URGP=0
PCworkstation kernel: [7671.387627] Iptables: SYN packet detectedIN=enp2s0 OUT=
MAC=1c:1b:0d:c1:96:59:ac:e0:10:f3:5d:47:08:00 SRC=291.235.112.122 DST=192.168.1.4 LEN=44 TOS=0x00

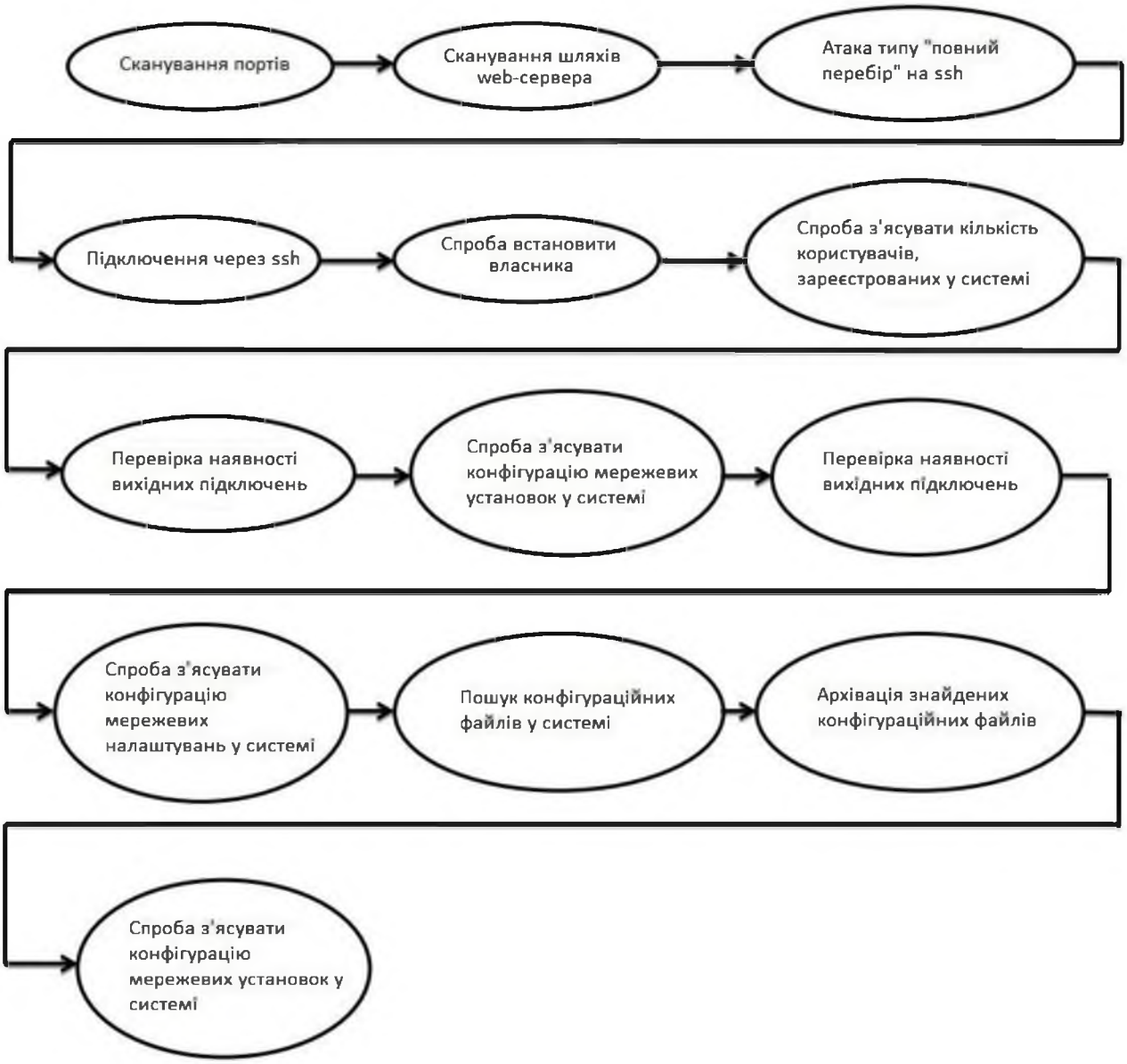
Продовження додатку Д.

PREC=0x00 TTL=46 ID=61665 PROTO=TCP SPT=51302 DPT=10215 WINDOW=1024 RES=0x00 SYN URGP=0 access.log 291.235.112.122 - - [20/May/2020:00:43:00 +0500] "GET /manual/da/nokia HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:43:02 +0500] "GET /manual/da/none HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:43:03 +0500] "GET /manual/da/processform HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:43:05 +0500] "GET /manual/da/process_order HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:43:08 +0500] "GET /manual/da/procure HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:43:10 +0500] "GET /manual/da/producers HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:03 +0500] "GET /manual/da/prodconf HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:04 +0500] "GET /manual/da/product_compare HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:05 +0500] "GET /manual/da/product_info HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:09 +0500] "GET /manual/da/product_thumb HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 89 Продолжение приложения В 291.235.112.122 - - [20/May/2020:00:44:12 +0500] "GET /manual/da/products HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:30 +0500] "GET /manual/da/products_new HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:31 +0500] "GET /manual/da/product-sort HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:38 +0500] "GET /manual/da/prog HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:41 +0500] "GET /manual/da/project HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:42 +0500] "GET /manual/da/promos HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:44 +0500] "GET /manual/da/promotions HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:45 +0500] "GET /manual/da/properties HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:44:49 +0500] "GET /manual/da/props HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:01 +0500] "GET /manual/da/pad HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:13 +0500] "GET /manual/da/page_sample1 HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:16 +0500] "GET /manual/da/page1 HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:17 +0500] "GET /manual/da/pagenotfound HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:18 +0500] "GET /manual/da/Pages HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:25 +0500] "GET /manual/da/paiement HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 291.235.112.122 - - [20/May/2020:00:45:34 +0500] "GET /manual/da/panelc HTTP/1.1" 404 434 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" sshd.log May 12 01:02:35 PCworkstation sshd[5756]: Failed password for Denis from 291.235.112.122 port 42108 ssh2 May 12 01:03:40 PCworkstation sshd[5755]: Failed password for Denis from 291.235.112.122 port 42106 ssh2 May 12 01:03:48 PCworkstation sshd[5762]: Failed password for Denis from 291.235.112.122 port 42114 ssh2 90 Продолжение приложения В May 12 01:04:06 PCworkstation sshd[5758]: Failed password for Denis from 291.235.112.122 port 42112 ssh2 May 12 01:04:22 PCworkstation sshd[5754]: Failed password for Denis from 291.235.112.122 port 42104 ssh2 May 12 01:04:45 PCworkstation sshd[5757]: Failed password for Denis from 291.235.112.122 port 42110 ssh2 May 12 01:05:03 PCworkstation sshd[5766]: Failed password for Denis from 291.235.112.122 port 42116 ssh2 May 12 01:05:29 PCworkstation sshd[5773]: Failed password for Denis from 291.235.112.122 port 42120 ssh2 May 12 01:05:31 PCworkstation sshd[5768]: Failed password for Denis from 291.235.112.122 port 42118 ssh2 May 12 01:05:33 PCworkstation sshd[5775]: Failed password for Denis from 291.235.112.122 port 42122 ssh2 May 12 01:05:55 PCworkstation sshd[5776]: Failed password for Denis from 291.235.112.122 port 42128 ssh2 May 12 01:06:01 PCworkstation sshd[5778]: Failed password for Denis from 291.235.112.122 port 42132 ssh2 May 12 01:06:02 PCworkstation sshd[5779]: Failed password for Denis from 291.235.112.122 port 42134 ssh2 May 12 01:06:40 PCworkstation sshd[5783]: Failed password for Denis from 291.235.112.122 port 42136 ssh2 May 12 01:06:41 PCworkstation sshd[5784]: Failed password for Denis from 291.235.112.122 port 42138 ssh2 May 12 01:07:12 PCworkstation sshd[5787]: Failed password for Denis from 291.235.112.122 port 42140 ssh2 May 12 01:07:58 PCworkstation sshd[5756]: Failed password for Denis from 291.235.112.122 port 42108 ssh2 May 12 01:08:22 PCworkstation sshd[5755]: Failed password for Denis from 291.235.112.122 port 42106 ssh2 May 12 01:08:34 PCworkstation sshd[5762]: Failed password for Denis from 291.235.112.122 port 42114 ssh2 May 12 01:08:45 PCworkstation sshd[5758]: Failed password for Denis from 291.235.112.122 port 42112 ssh2 May 12 01:09:16 PCworkstation sshd[5754]: Failed password for Denis from 291.235.112.122 port 42104 ssh2 May 12 01:10:13 PCworkstation sshd[5766]: Failed

Продовження додатку Д.

password for Denis from 291.235.112.122 port 42116 ssh2 May 12 01:10:22 PCworkstation sshd[5773]: Failed password for Denis from 291.235.112.122 port 42120 ssh2 May 12 01:10:31 PCworkstation sshd[5768]: Failed password for Denis from 291.235.112.122 port 42118 ssh2 91 Продолжение приложения В May 12 01:10:32 PCworkstation sshd[5757]: Failed password for Denis from 291.235.112.122 port 42110 ssh2 May 12 01:10:51 PCworkstation sshd[5775]: Failed password for Denis from 291.235.112.122 port 42122 ssh2 May 12 01:10:56 PCworkstation sshd[5776]: Failed password for Denis from 291.235.112.122 port 42128 ssh2 May 12 01:11:32 PCworkstation sshd[5778]: Failed password for Denis from 291.235.112.122 port 42132 ssh2 May 12 01:12:15 PCworkstation sshd[5779]: Failed password for Denis from 291.235.112.122 port 42134 ssh2 May 12 01:13:21 PCworkstation sshd[5783]: Failed password for Denis from 291.235.112.122 port 42136 ssh2 May 12 01:15:25 PCworkstation sshd[5784]: Failed password for Denis from 291.235.112.122 port 42138 ssh2 May 12 01:15:30 PCworkstation sshd[5783]: Accepted password for Denis from 291.235.112.122 port 42136 ssh2

ДОДАТОК Е. Зображення моделюється атаки



ДОДАТОК Є. Перелік документів на оптичному носії

1 Титульна сторінка.docx

2 Завдання.docx

3 Реферат.docx

4 Список умовних скорочень.docx

5 Зміст.docx

6 Вступ.docx

7 Стан питання. Постановка задачі.docx

8 Спеціальна частина.docx

9 Економічний розділ.docx

10 Висновки.docx

11 Перелік посилань.docx

12 Додаток А.docx

13 Додаток Б.docx

14 Додаток В.docx

15 Додаток Г.docx

16 Додаток Д.docx

17 Додаток Е.docx

18 Додаток Є.docx

19 Додаток Ж.docx

20 Додаток З.docx

Презентація.pptx

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Аналіз та підвищення рівня захищеності інтернет-мережі підприємства «ЯВІР ДНІПРО-1»
студента групи 125м-22-1
Хіблін Миколи Миколайовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 117 сторінках та містить 24 рисунки, 13 таблиць, 22 джерела та 9 додатків.

У вступній частині роботи автор приділяє увагу аналізу та дослідженню існуючої інформаційної безпеки при роботі в інтернет-мережах на підприємстві «ЯВІР ДНІПРО-1».

У спеціальному розділі дипломної роботи приведено комплекс організаційних заходів забезпечення інформаційної безпеки та захисту інформації підприємства. Наведені результати щодо ефективності використання системи в конкретних умовах та рекомендації щодо вибору та впровадження систем забезпечення інформаційної безпеки для підприємства.

В економічному розділі розрахована вартість та рентабельність впровадження щодо підвищення рівня захищеності інтернет-мережі «ЯВІР ДНІПРО-1» та капітальні витрати.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам "Положення про систему виявлення та запобігання плагіату".

Як зауваження необхідно відзначити деякі стилістичні неточності та недостатню проробку окремих питань.

В цілому кваліфікаційна робота заслуговує оцінки «_____», а її автор присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини,
асистент кафедри БІТ **Ю.П. Рибальченко**

Керівник роботи,
к.ф.-м.н., проф. кафедри БІТ **О.Ю. Гусєв**

ДОДАТОК З. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 87 б. («Вісімдесят сім»).

Керівник розділу доц. Пілова Д.П.