Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка
до дипломного проєкту (роботи)
магістр
(ступінь вищої освіти)

на тему Аналіз рівня захисту інформації в лініях зв'язку комп'ютерних мереж
(назва теми)

Виконав(ла): студент(ка) IIм курсу,
групи БК-812м
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем
АГЕЙЧИК Д.Ю.
(ПРІЗВИЩЕ та ініціали)

Керівник ЛІЗУНОВ С.І.
(ПРІЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРІЗВИЩЕ та ініціали)

2023

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
Андрій КОРОТУН
«____» _____2023року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

АГЕЙЧИКА Даніїла Юрійовича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз рівня захисту інформації в лініях зв'язку комп'ютерних мереж
Analysis of the level of information security in computer interconnection lines

керівник проєкту (роботи) к.т.н., доцент ЛІЗУНОВ Сергій Іванович,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «28» листопада 2023 року №475
2. Строк подання студентом проєкту (роботи) 11.12.2023
3. Вихідні дані до проєкту (роботи) аналіз рівня захищеності інформації в комп'ютерних мережах.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) загрози безпеці інформації в лініях зв'язку комп'ютерних мереж, апаратне та програмне забезпечення захисту ресурсів мережі, оцінка ризиків у комп'ютерних мережах, безпека на межі мережі: архітектура розподіленого брандмауера.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 12 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	ЛІЗУНОВ С.І., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання «04» вересня 2023року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Систематизація літературних джерел. Аналіз літературних джерел за тематикою дослідження.	04.09.23 – 18.09.23	виконано
2.	Складання і затвердження наукового завдання.	19.09.23 – 24.09.23	виконано
3.	Формування та уточнення наукового завдання.	25.09.23 – 27.09.23	виконано
4.	Загрози безпеці інформації в лініях зв’язку комп’ютерних мереж.	27.09.23 – 28.09.23	виконано
5.	Апаратне та програмне забезпечення захисту ресурсів мережі.	29.09.23 – 15.10.23	виконано
6.	Оцінка ризиків у комп’ютерних мережах критичної інфраструктури.	16.10.23 – 31.10.23	виконано
7.	Архітектура брандмауера.	01.11.23 – 19.11.23	виконано
8.	Оформлення матеріалів магістерської роботи.	20.11.23 – 30.11.23	виконано

Студент(ка) _____ Даніїл АГЕЙЧИК
(підпис) (Ім’я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Сергій ЛІЗУНОВ
(підпис) (Ім’я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 63 с., 11 рис., 77 джерел.

БЕЗПЕКА МЕРЕЖІ, БРАНДМАУЕРИ, КОМП'ЮТЕРНІ МЕРЕЖІ, КРИТИЧНА ІНФРАСТРУКТУРА, РИЗИКИ

Мета роботи: проналізувати рівень захисту інформації в комп'ютерних мережах.

Об'єкт та предмет дослідження: об'єктом дослідження виступають комп'ютерні мережі; предметом дослідження є рівень захисту інформації в комп'ютерних мережах.

Методи дослідження: описово-аналітичний.

Результати: результатом дослідження є визначення основних загроз безпеці інформації в лініях зв'язку комп'ютерних мереж та представлення методів розрахунку їх стійкості.

Рекомендації щодо впровадження: робота носить фундаментальний характер, проте деякі її результати можуть бути використані при розробці нових методів захисту інформації в лініях зв'язку комп'ютерних мереж.

Практична цінність: представлені способи оцінки ефективності захисту, які можна здійснити на основі аналізу відповідних ризиків і шансів.

ABSTRACT

Explanatory note to the master's thesis: 63 pp., 11 fig., 77 sources.

COMPUTER NETWORKS, CRITICAL INFRASTRUCTURE, FIREWALLS, NETWORK SECURITY, RISKS

The purpose of the work: to analyze the level of information protection in computer networks.

Object and subject of research: the object of research is computer networks; the subject of research is the level of information protection in computer networks.

Research methods: descriptive and analytical.

Results: the result of the study is the determination of the main threats to information security in the communication lines of computer networks and the presentation of methods for calculating their stability.

Recommendations for implementation: the work is of a fundamental nature, but some of its results can be used in the development of new methods of information protection in communication lines of computer networks.

Practical value: methods of assessing the effectiveness of protection are presented, which can be carried out based on the analysis of the relevant risks and chances.

ЗМІСТ

ВСТУП

Безпека мережі є одним із найважливіших аспектів у сфері інформаційної безпеки сьогодні із розширенням залежності бізнес-системи від IT-інфраструктури. Відсутність заходів безпеки в IT-інфраструктурі може завдати непоправної шкоди організаціям і компаніям, що є небажаним для бізнесу та маркетингового процессу.

Метою безпеки мережі є в першу чергу запобігання збитку від неправильного використання даних. Існує ряд потенційних проблем, які можуть виникнути, якщо захист мережі не реалізовано належним чином. Кожна компанія повинна буде захистити певну важливу та секретну інформацію від доступу своїх конкурентів. Втрата даних може знизити додану вартість у процесі виробництва деталей і маркетингу. Крім того, справжній шлях у бізнесі та маркетингу продукту може бути втрачений через маніпуляції даними в результаті відсутності заходів безпеки у фінансовій інформації. Як наслідок, відсутність заходів безпеки в мережі даних може призвести до порушення конфіденційності в різних бізнесах і маркетингу продуктів. Тому для будь-якого адміністратора мережі життєво важливо використовувати суворі політики для запобігання потенційним втратам, незалежно від розміру та типу мережі [1]. Це набір політик, правил і домовленостей, розроблених мережевим адміністратором або адміністраторами для запобігання та моніторингу несанкціонованого доступу, неправильного використання, виправлення, запобігання змінам або обмеження доступу до комп’ютерних мереж і мережевих ресурсів [2].

З огляду на вищенаведене, тема роботи є актуальною.

1 ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ В ЛІНІЯХ ЗВ'ЯЗКУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Загрози мережевій безпеці та атаки

Щоб забезпечити заходи безпеки в мережі даних, атаки повинні бути чітко визначені. Атака — це небезпечна або небезпечна спроба змінити або використати ресурс, доступний через мережу, у непередбачений спосіб. Мережеві атаки можна розділити на три загальні категорії:

1. Несанкціонований доступ до ресурсів та інформації через мережу.

2. Несанкціоноване маніпулювання інформацією в мережі.

3. Атаки, які призводять до порушення надання послуг і називаються відмовою в обслуговуванні [3].

Ключове слово в перших двох категоріях - вчиняти дії протиправно. Визначення авторизованої чи несанкціонованої дії є відповідальністю політики безпеки мережі, яку можна визначити як спробу користувача переглянути або змінити інформацію, що заборонено. Неавторизований доступ може бути однією з найпоширеніших атак на будь-яку мережу. Таким чином зловмисник намагається отримати доступ до закритої зони інформації та мережі. Злам паролів, створення підшляхів, створення підроблених ідентифікацій або використання шкідливих програм є основними способами здійснення цих атак [4, 5].

Знищення інформації є однією з найбільш руйнівних мереж атак. Таким чином зловмисник намагається знищити певну інформацію, виконуючи команди в базі даних. Це може бути обмеженим або дуже широким. Залежно від типу зловмисника мережа може втратити всю вашу інформацію за лічені секунди. Ще однією формою несанкціонованого доступу є атаки, які призводять до порушення надання послуг. У цьому методі особа входить в область користувача або керування, щоб виконати команду або набір команд, які зазвичай заборонені. Таким чином зловмисник

може писати, змінювати, надсилати електронну пошту, копіювати або видаляти певну інформацію, щоб знайти спосіб отримати доступ до обмежених даних. Масштаб атаки залежить від можливостей зловмисника [6,7].

Загрози мережевій безпеці належать до однієї або двох загальних категорій, як атаки на логіку або атаки на регрес. Раціональні атаки, як випливає з назви, є прибутковою стратегією, яка використовується для усунення будь-яких слабких місць у системі. Слабкі сторони можуть включати уразливості програмного забезпечення, такі як бекдори та помилки безпеки в коді [8]. Метою атаки є проникнення в систему з метою пошкодження або отримання несанкціонованого доступу до системи [9]. Атаки на ресурси спрямовані на знищення ресурсів мереж. Трюк став більш популярним у 1990-х роках, але поступово впав у популярності. У цьому методі мережева система змушена бути зруйнована, тому вона є вразливою. Ці атаки здійснюються різними способами, щоб застосувати силу до мережі даних. Найшвидший спосіб — це для сервера зіткнутися з величезним потоком запитів на обслуговування, які знаходяться поза його контролем. Крім того, деякі атаки на ресурси передбачають встановлення шкідливого програмного забезпечення в мережі, що робить її вразливою [10].

Існує також інша класифікація різних атак на захищені мережі:

– Пасивні атаки: пасивні атаки спрямовані проти безпеки мережі організації з метою ідентифікації мережі; зловмисник стежить за мережею організації. Оскільки під час цієї атаки зловмисник не виконує жодних зловмисних дій для виявлення цього типу атаки, це дуже важко, наприклад, один тип пасивної атаки полягає в тому, що зловмисник захоплює пакети внутрішньої мережі організації, сподіваємось, що це типу атаки можна легко запобігти за допомогою належного шифрування в мережевій інфраструктурі [11].

– Активні атаки: у цьому типі атаки зловмисник безпосередньо атакує сервери організації. Атаки видимі для систем безпеки мережі, щоб їх можна

було контролювати. Стратегії боротьби з цими атаками включають встановлення брандмауерів (програмного та апаратного забезпечення), а також систем IPS [11, 12].

– Внутрішні атаки: (зблизька) у цьому типі атаки зловмисники мають фізичний доступ до систем. На жаль, маючи фізичний доступ до систем, майже будь-який зловмисник може зробити багато роботи та завдати непоправної шкоди організації. Відповідним і логічним способом боротьби з цим типом атак є забезпечення фізичної безпеки систем і серверів [12].

– Внутрішні атаки: ці типи мережевих атак зазвичай здійснюються внутрішніми користувачами організацій, які мають доступ до систем та інформації. Відповідно до рівня знань та поінформованості зловмисників на комп'ютерні мережі, вони можуть проникати в мережеві системи. Рішення атак полягає в тому, щоб запобігти цьому типу атак безпеки на Рівні 2 і зосередитися на автентифікації, тоді як фізична безпека повинна бути повністю забезпечена [12, 13].

1.2 Заходи безпеки

Щоб надати базові знання про заходи безпеки в мережі даних, у цьому розділі представлено деякі концепції безпеки мережі. У сучасній мережі є багато ресурсів для захисту. Нижче наведено список мережевих ресурсів, які слід захищати від усіх типів атак:

1. Брандмауери, маршрутизатори та комутатори як мережеве обладнання.

2. Інформація про роботу мережі, така як таблиці маршрутизації та конфігурації списків доступу, що зберігаються на маршрутизаторі.

3. Нематеріальні ресурси мережі, такі як пропускна здатність і швидкість.

4. Інформація та інформаційні ресурси, підключені до мережі, такі як бази даних та інформаційні сервери.

5. Термінали, підключені до мережі для використання різних джерел.

6. Інформація, що обмінюється в мережі в будь-який момент часу.

7. Зберігання операцій користувачів і використання їх мережевих ресурсів конфіденційними для запобігання ідентифікації користувачів [14, 15].

На підключених до мережі комп'ютерах, таких як база даних і веб-сервери, відбувається обмін інформацією через мережу та інформацією про мережеві компоненти для виконання таких завдань, як таблиці маршрутизації маршрутизатора. Мережевими ресурсами також може бути термінальне обладнання, таке як маршрутизатори та брандмауери або механізми підключення, щоб запобігти доступу хакерів до захищених даних [16].

Принципи проектування мережевої безпеки: щоб запровадити вдосконалені системи безпеки в мережі даних, належний метод проектування та принципи повинні бути застосовані до заходів безпеки мереж. Захист мережевої безпеки є першою лінією захисту системних ресурсів інформаційних технологій (IT) від загроз (таких як зловмисники або зловмисний код), які виникають із потоків поза мережею. Основні заходи захисту для безпеки мережі включають брандмауери, виявлення вторгнень і брандмауер веб-додатків, систему виявлення вторгнень (IDS) і систему запобігання вторгненням (IPS), захист віртуальної приватної мережі (VPN) і системи перевірки вмісту, такі як антивірус, захист від зловмисного програмного забезпечення, антиспам і фільтрація Uniform Resource Location (URL) [17]. Ці апаратні та програмні рішення підтримують і доповнюють механізми безпеки для операційних систем, баз даних і програм. Щоб забезпечити ефективну систему безпеки в захищених даних мереж, застосовуються передові методи проектування блок-схем щодо рівнів загроз [18]. Основні принципи безпеки IT-систем, які слід враховувати при проектуванні системи безпеки мережі, наведені на рис. 1.1 [19]. Політика

безпеки: політика безпеки мережі повинна бути визначена таким чином, щоб мінімізувати ризик і розмір збитків після аналізу ризиків у мережі даних. Політика безпеки має бути загальною і в полі загального бачення, а не вдаватися в деталі. Деталі можуть змінитися протягом короткого часу, але загальні принципи безпеки мережі, які складають її політики, залишаються незмінними [20].

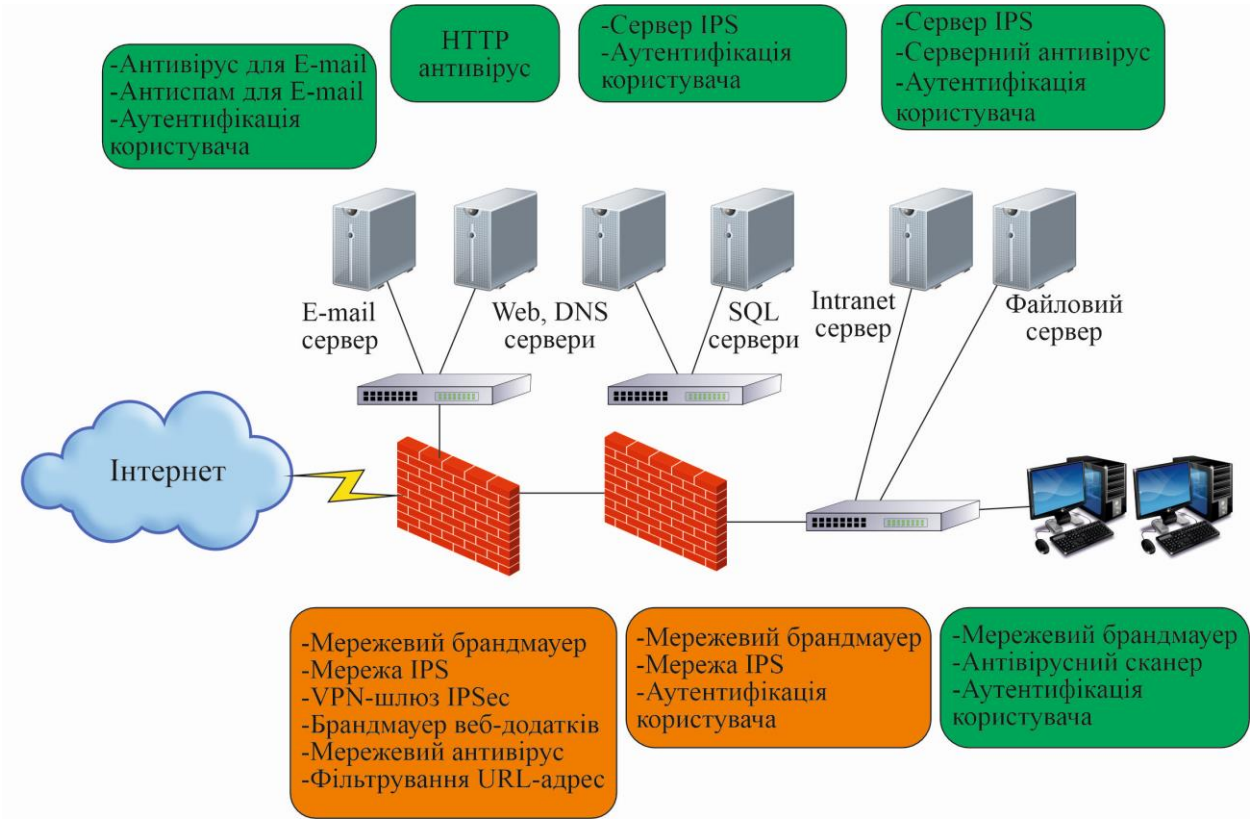

Рисунок 1.1 – Принцип комплексного захисту: захист різних ресурсів IT-системи на основі кількох взаємодоповнюючих рівнів безпеки [19]

Елементами політики безпеки є:

1. Що і чому дані слід захищати.
2. Хто відповідає за захист даних.
3. Створення контексту, який вирішує будь-які можливі конфлікти.
4. Політики безпеки можна загалом розділити на дві категорії:
5. Дозвільна: дозволено все, що конкретно не заборонено.
6. Обмежувальний: все, що явно не дозволено, заборонено.

Зазвичай ідея використання обмежувальних політик безпеки є кращим і більш відповідним методом з точки зору підвищення безпеки мережевих систем. Цей вибір викликаний проблемами безпеки авторизованих політик, щоб забезпечити обмеження доступу до захищених даних [21,22].

Найкращий підхід до впровадження надійної безпеки мережі – мати мережу повністю підготовленою до загроз. Ось чотири поради щодо впровадження безпеки мережі:

1. Безпека: переконайтеся, що всі компоненти належним чином ліцензовані та мають політики автентифікації та захисту.
2. Огляд: відстежуйте діяльність мережі та безперервність дій захисту.
3. Тестування: Оцініть вразливі місця політик безпеки, призначених для мережі, імітуючи атаку довіреної особи. Якщо вдасться обійти заборони, доведеться застосовувати більш складні методи.
4. Покращення ситуації: на основі всіх попередніх кроків збирайте дані та використовуйте їх для створення кращих заходів [23, 24].

Усі адміністратори мережі повинні пам’ятати, що хороша стратегія безпеки мережі передбачає постійний моніторинг і обслуговування. Звичайно, недостатньо, щоб політики безпеки були створені та залишені, щоб виконувати свою роботу. Зловмисники постійно оновлюють себе, щоб знайти шлях до захищених даних. Отже, мережеві адміністратори повинні бути в курсі цих удосконалень [25].

Усунення небезпеки: після визначення мережевих активів та їх загрозливих факторів слід оцінити різні ризики. У кращому випадку мережа повинна захищати від усіх видів помилок, але дешевої безпеки не досягти. Тому необхідно правильно оцінити типи ризиків, щоб визначити найважливіші з них, а з іншого боку, визначити джерела, які слід захистити від цих ризиків. Двома основними факторами в аналізі ризику є:

1. Можливість здійснення атаки.
2. Пошкодження мережі в разі успішної атаки [26, 27].

Рівні безпеки – це класифікація мережевих дій, завдяки чому кожну мережеву діяльність можна захищати окремо, а політики безпеки одного рівня не впливають на параметри безпеки іншого рівня. Наприклад, якщо атака DOS у сфері мережевої безпеки відбувається на рівні безпеки на стороні користувача, ми не прагнемо боротися з цією атакою на рівні управління [28]. Рівні безпеки мережі дають змогу досліджувати безпеку кожної діяльності окремо шляхом класифікації мережевих дій та розміщення їх на різних рівнях. Оскільки кожна діяльність розглядається окремо, заходами безпеки на кожному рівні можна точно керувати. Служба VoIP на рівні безпеки служби, безпека керування послугами (така як безпека користувача), безпека незалежного від контролю служби (така як протокол SIP) і безпека даних на стороні користувача (така як голос користувача) є деякими прикладами застосування рівень безпеки мережі в заходах безпеки мереж [29], [30]. Щоб підвищити рівень безпеки комплексної IT-інфраструктури, відповідні рішення безпеки будуть використовуватися на всіх рівнях IT-архітектури підприємства. Щоб встановити наскрізну безпеку, необхідно застосувати компоненти безпеки, пов’язані з різним обладнанням і групами. Завданням рівнів безпеки, як і мережевих рівнів, є надання послуг і активація вищого рівня. Таким чином, у мережі даних відчувається потреба в мережевому шаруванні. Розглядаються три рівні безпеки, і шляхом визначення різних рівнів безпеки пропонується ієрархічне рішення для безпеки мережі. Розрівнювання виконується таким чином, що кожен рівень має власні вразливості, що робиться з метою полегшення боротьби із загрозами [31].

«Рівень безпеки інфраструктури» вмикає «Рівень безпеки служби», а цей рівень також увімкне «Рівень безпеки додатків», щоб забезпечити розширену безпеку мережі за допомогою мережевих рівнів. Наступні шари пояснюються як

– Рівень безпеки інфраструктури: Рівень інфраструктури охоплює безпеку об’єктів мережі передачі, а також окремих мережевих інструментів.

Цей рівень забезпечує опис основних мережевих реалізацій, послуг і додатків кожного [32].

– Рівень безпеки послуг: на цьому рівні забезпечується безпека послуг, які постачальники послуг надають клієнтам. Цей діапазон послуг включає базові послуги (наприклад, послуги Інтернет-зв'язку, такі як сервер автентифікаційного обліку авторизації (AAA), служба системи доменних імен (DNS) тощо) до спеціальних служб, таких як голос через Інтернет-протокол (VOIP), VPN тощо Завданням цього рівня є захист постачальників послуг та їхніх клієнтів від потенційних загроз безпеці [32].

– Рівень безпеки програми: цей рівень зосереджений на програмах, які доступні для користувачів в Інтернеті. Мережеві програми можуть надаватися постачальниками послуг додатків (ASP) як сторонніми постачальниками, самим постачальником послуг як ASP або їх хост-компаніями, які мають незалежний центр обробки даних. Відповідно на цьому рівні чотири цілі можна розглядати як загрозу: 1- користувачі програми, 2- постачальник програми, 3-суб-провайдер 4- постачальник послуг [33]. Структура прикладного рівня безпеки в мережевій безпеці та завдання кожного розділу наведено на рис. 1.2 [33].

Рисунок 1.2 - Застосування рівня безпеки в системі безпеки мережі [33]

– Контроль рівня безпеки: функція цього рівня полягає в підтримці діяльності, яка відповідає за передачу інформації про служби або мережеві програми. Цей рівень, як правило, включає зв'язок між машинами в мережі, який зазвичай включає в себе повідомлення керування [33].

– Рівень безпеки на стороні користувача: цей рівень включає захист доступу та використання послуг, які надає провайдер на стороні користувача. Кінцеві користувачі можуть використовувати саму мережу постачальника послуг або додаткові служби, такі як VPN, або в мережах на основі додатків [33].

– Сегментація інформації: ресурси IT-системи з різними рівнями чутливості, включаючи толерантність до ризику та вразливість до різного ступеня загрози, повинні бути включені в різні зони безпеки. Принцип «приховування інформації» розглядається як один із розширених випадків цього правила, так що IT-системи надають лише ті дані, які необхідні для виконання завдань IT-системи. Система може бути представлена як сервери для Інтернет-провайдерів, які зареєстровані лише в публічному DNS. Принцип мінімальних балів. Люди, підключені до IT-системи (наприклад, користувачі та системні адміністратори), повинні мати мінімальні привілеї, необхідні для оптимальної продуктивності в організації. Це також стосується даних і послуг, які надаються зовнішнім користувачам. Одним із розширень цього правила є принцип «необхідності знати», згідно з яким користувачі та менеджери IT-систем мають доступ лише до інформації, що стосується їхніх ролей та завдань [34].

Рівень безпеки IT-системи залежить від фактора, який має найменшу захищеність. Одним із розширень цього правила є принцип єдиної точки відмови (SPOF), який пов’язаний із доступністю мережевих служб, згідно з яким усі зв’язки, обладнання (мережеве та безпекове), а також сервери на мережевих маршрутах між користувачами і продуктивність IT-системи важливих ресурсів повинна бути реалізована в резервованих конфігураціях. При проектуванні системи безпеки мережі слід враховувати принципи

організаційної безпеки, включаючи правила «розподілу обов'язків» і «робочого процесу». Метою цих принципів є обмеження можливості співробітників ігнорувати та порушувати політику безпеки ІТ-системи. Розподіл обов'язків означає, що важливі завдання та функції повинні виконуватися двома або більше працівниками [35]. Крім того, слід враховувати плинність робочих місць для важливих посад з точки зору заходів безпеки мереж. Ресурси ІТ-систем з різними рівнями чутливості повинні розташовуватися в різних зонах безпеки. Постачальники комп’ютерного обладнання та послуг для зовнішніх мереж (наприклад, компанії-провайдери Інтернету) повинні розташовуватися в різних областях (наприклад, у демілітаризованій зоні), на відміну від комп’ютерних систем і внутрішнього мережевого обладнання. Стратегічні ресурси ІТ-системи повинні бути розташовані в певних зонах безпеки, щоб бути захищеними [36]. Низьконадійне комп’ютерне обладнання та системи, такі як сервери віддаленого доступу та точки доступу до бездротової мережі, також повинні бути включені до окремих зон безпеки. Різні типи ресурсів ІТ-системи слід розміщувати в окремих зонах безпеки. Робочі станції для користувачів повинні бути розташовані в різних зонах безпеки, на відміну від серверів. Системи безпеки та управління мережею повинні бути розташовані в певних зонах безпеки. Системи на етапі розробки повинні бути розташовані в іншому секторі, на відміну від систем, пов’язаних із етапом виробництва [37].

1.3 Запобігання вторгненням і брандмауери

Брандмауери в програмних або апаратних системах діють як стіна безпеки між користувачами мереж і зовнішнім світом. Брандмауери зазвичай розташовані на кордоні між нашою мережею та Інтернетом. Апаратні

брандмауери можуть контролювати вміст і шляхи зв’язку нашої мережі. Брандмауери визначають правила того, як інформація надходить і виходить з нашої мережі та Інтернету. Насправді ми використовуємо брандмауери, щоб визначити, які дані мають право на вхід і вихід, а які ні [38], [39]. Програмні брандмауери є економічно ефективними інструментами в системах брандмауерів, і вони можуть досліджувати шаблони та вміст і можуть трохи контролювати загрози. Крім того, апаратні брандмауери є дуже потужними і тому можуть використовуватися більше, ніж їх програмні режими [40], [41]. На розсуд користувача брандмауер є основним інструментом для підтримки або обмеження потоку мережевого трафіку в різних ситуаціях, таких як спеціальне обладнання брандмауера, функція брандмауера в обладнанні IPS і список контролю доступу в мережевих комутаторах і маршрутизаторах. При правильному розгортанні та конфігурації брандмауери можуть допомогти побудувати безпечні архітектури, розділити інфраструктуру IT-мережі на домени безпеки та контролювати зв’язок між ними [42].

Щоб посилити кібератаку на захищені дані, [43] розроблено передову IDS. У цій статті представлено вдосконалене моделювання кібератак, щоб запобігти доступу хакерів до захищених даних у мережах. Віруси, хробаки та трояни намагаються поширитися мережею та можуть залишатися на безсимптомних заражених пристроях протягом кількох днів або тижнів. Наша робота полягає в тому, щоб докласти заходів безпеки, щоб запобігти проникненню цього типу шкідливих програм, а також шкідливих програм, які відкривають їм шлях.

Реалізація процесу безпеки мережі для запобігання вторгненню шляхом контролю обмеженого доступу користувачів до внутрішньої мережі показано на рис. 1.3 [19]. У цьому прикладі Інтернет-послуги для внутрішніх користувачів доступні лише через корпоративну електронну пошту та проксі-сервери протоколу передачі гіпертексту (HTTP).

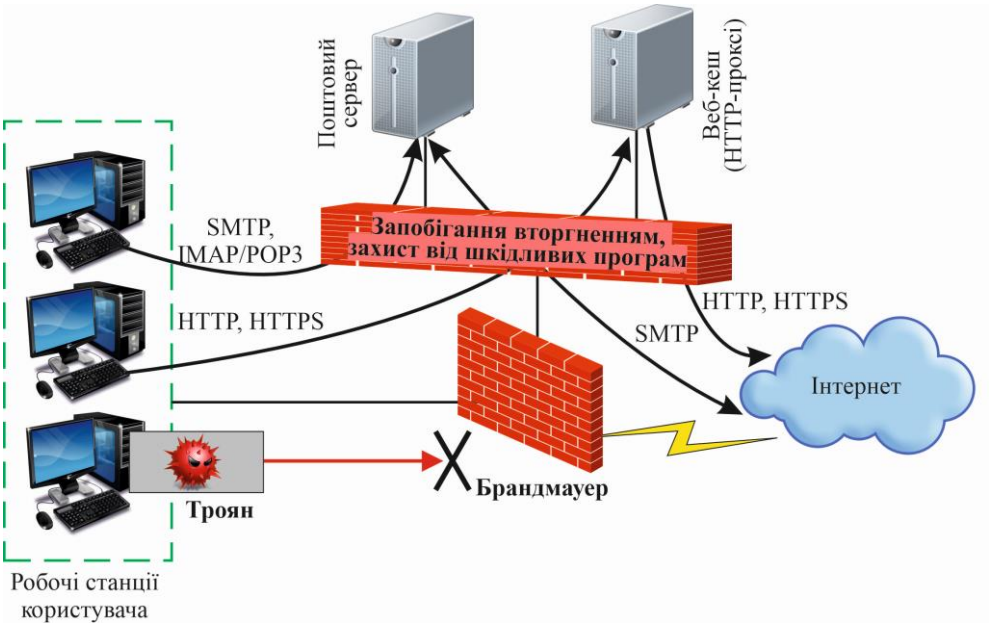

Рисунок 1.3 – Запобігання вторгненню шляхом контролю обмеженого доступу користувачів до внутрішньої мережі [19]

1.4 Організація безпеки мережі

Загальна стратегія в цьому випадку складається з трьох кроків. Насправді безпека мережі включає в себе наступне:

1- Захист: потрібно правильно налаштувати системи та мережу.

2- Виявлення: потрібно повністю контролювати мережу та виявляти зміни та використання мережевих ресурсів, які є ознаками вторгнення.

3- Реакція: після виявлення проблем потрібно швидко на них реагувати та швидко забезпечити безпечне середовище в мережі [44].

Це стратегія захисту від нападників. Якщо серед експертів з безпеки є один спільний знаменник, то небезпечно покладатися на першу єдину лінію захисту. Тому що будь-який засіб захисту може бути знищений ворогом. Мережа – це не лінія чи точка, яка насправді є територією. У результаті, якщо зловмисник атакував частину захищених даних, можна зберегти ресурси даних і врятувати їх, якщо система безпеки належним чином

організована для техніки захисту [45]. Рішення безпеки мережі можна представити наступними кроками:

1- Оцінка ризиків і вразливостей і аналіз вибору відповідних контролерів.

2- Оптимізація серверів, клієнтів, веб-сайтів і мережевого середовища організації.

3- Оптимізація кешу, трансляції мережевих адрес (NAT), проксі, адрес Інтернет-протоколу (IP) і мереж маршрутизації.

4- Поради щодо вибору правильних стандартів безпеки.

5- Поради щодо визначення та застосування керівних принципів та виконавчих інструкцій щодо інформаційної безпеки.

6- Навчання на місці або періодично на різних рівнях.

7- Перевірка міцності систем безпеки, намагаючись їх зламати.

Безпека мережі – це процес, у якому мережа захищена від різних типів внутрішніх і зовнішніх загроз. Метою безпеки мережі є захист мережі від вищевказаних атак, тому цілі можна представити в трьох категоріях:

1. Підтвердження конфіденційності даних.
2. Підтримка повних даних.
3. Підтримка доступності даних.

Розумними є наступні кроки для забезпечення безпеки:

1. Визначення частини, яку слід захистити.
2. Вирішення випадків, від яких потрібно захищати відповідний розділ.
3. Вирішення способів погроз.
4. Впровадження засобів які можуть захистити ваші активи економічно ефективним способом.
5. Постійний перегляд процесу та посилення його у разі слабкості. Визначаючи політику безпеки, ми досягаємо її реалізації у вигляді плану безпеки мережі. Елементи, які складають план безпеки мережі:

1. Функції безпеки кожного пристрою, такі як пароль адміністратора або використання Secure Shell (SSH).
2. Брандмауери.

3. Інтегратори VPN для віддаленого доступу.
4. Виявлення вторгнень.
5. AAA сервери безпеки та інші служби AAA для мережі.
6. Контроль доступу та механізми обмеження доступу для різних мережевих пристроїв.

Щоб підвищити безпеку різних систем, передову мережу систем безпеки можна об’єднати разом, щоб поділитися перевагами кожної системи в різних місцях. Розширена система моніторингу техніки безпеки може бути реалізована, щоб зменшити швидкість вторгнення в захищені дані. Необхідно надати нові протоколи та правила для заходів безпеки різних організацій щодо нових рівнів атак на мережі, щоб захистити дані. Отже, для підвищення рівня безпеки в мережах необхідно представити нове рішення щодо розроблених загроз. Апаратне забезпечення систем безпеки мережі можна модифікувати, щоб забезпечити розширені заходи безпеки в мережі даних. Нове програмне забезпечення брандмауера щодо розроблених методів хакерів може бути представлено для того, щоб забезпечити ключовий інструмент у системах захисту даних. Удосконалена модель апаратного процесора та системи зв’язку програмного забезпечення для виявлення та запобігання мережевим атакам може бути реалізована в рамках процесу підвищення безпеки мережі. У результаті може бути представлена передова система безпеки мережі, щоб зменшити рівень доступу до даних з боку хакерів.

2 АПАРАТНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ РЕСУРСІВ МЕРЕЖІ

У зв’язку з «багатокористувацьким» режимом роботи в комп’ютерній мережі виникає цілий комплекс взаємопов’язаних питань щодо захисту інформації, що зберігається на комп’ютерах або серверах комп’ютерної мережі [1, 2].

Слід зазначити, що самі мережеві операційні системи також забезпечують потужний захист від несанкціонованого доступу до мережевих ресурсів. Однак бувають випадки, коли навіть такий захист не працює. Практика показує, що неавторизований користувач з достатнім досвідом у сфері системного та мережевого програмування, який задумав підключитися до мережі, навіть маючи обмежений доступ до певних ресурсів, рано чи пізно все одно може отримати доступ до деяких захищених ресурсів мережі. Тому виникає необхідність у створенні додаткового апаратного та програмного забезпечення для захисту ресурсів мережі.

До засобів апаратного захисту відносяться різноманітні брандмауери, фільтри, пристрої шифрування протоколів і т. д. До програмних засобів захисту належать: програми шифрування даних; програми відстеження мережевих підключень (моніторинг мережі); програми автентифікації та ідентифікації та ін. При розробці масштабних комп'ютерних мереж виникає проблема забезпечення взаємодії великої кількості комп'ютерів і серверів, тобто проблема пошуку оптимальних топологій. Найважливішою складовою локальних і корпоративних мереж є їх системна топологія, яка визначається архітектурою міжкомп’ютерних з’єднань [3–4].

Відомо, що критична інформація повинна оброблятися в комп'ютерних мережах для забезпечення безпеки.

Термін «критична інформація» відноситься до інформації: з різними грифами секретності; інформація для службового користування; відомості,

що становлять комерційну таємницю або таємницю підприємства; відомості, які є власністю певної організації або особи.

Наведемо деякі основні визначення. Вплив — це форма можливої втрати або пошкодження комп’ютерної мережі. Наприклад, викриття вважається несанкціонованим доступом до даних або протидією авторизованому використанню комп’ютерної мережі. Уразливість — це слабка сторона безпеки, яка може спричинити пошкодження комп’ютерної мережі.

Атака - це дія якогось суб'єкта комп'ютерної мережі, яка використовує вразливість комп'ютерної мережі для досягнення цілей, що виходять за межі авторизації цього суб'єкта в комп'ютерній мережі. Загроза для комп’ютерної мережі – це стан, який потенційно може завдати шкоди комп’ютерній мережі.

Управління в термінології безпеки - це захисний механізм (дія, пристрій, процедура, технологія тощо), який зменшує вразливість комп’ютерної мережі.

Кожен вузол мережі є незалежною комп'ютерною системою з усіма притаманними їй проблемами, а також є проблеми, пов'язані з лініями зв'язку і процедурою передачі інформації. З точки зору безпеки комп'ютерні мережі мають такі недоліки: - спільне використання ресурсів. Оскільки ресурси та навантаження розподіляються між різними вузлами мережі, багато користувачів мають потенціал отримати доступ до мережі як єдиної комп’ютерної системи. Іншими словами, отримавши доступ до однієї з систем, що входять в мережу, користувач (або зловмисник) має реальну можливість атакувати інші системи мережі; - складність системи. Кожна комп’ютерна система має операційну систему, яка є складним набором взаємодіючих програм.

Через цю обставину важко сформулювати чіткі вимоги безпеки, особливо для мереж загального призначення, які були розроблені без урахування безпеки; – невизначена периферія

На вразливість мережі сильно впливає неможливість визначити, у більшості випадків, точні межі мережі. Один і той же вузол може одночасно працювати в декількох мережах, і, отже, ресурси однієї мережі цілком можуть використовуватися з вузлів, що входять до складу іншої мережі. Такий широкий розподіл ресурсів, безсумнівно, є перевагою.

Однак невизначена кількість потенційно непідготовлених користувачів і потенційних загарбників значно ускладнює безпеку як мережі в цілому, так і більшості її окремих вузлів; - кілька точок атаки. В одній комп'ютерній системі можна контролювати доступ користувачів до системи, оскільки доступ забезпечується з терміналів комп'ютерної системи.

Зовсім інша ситуація в мережі: один і той же файл може бути запрошений так званим віддаленим доступом з різних вузлів мережі. Отже, якщо адміністратор конкретної системи може проводити чітку політику безпеки по відношенню до своєї системи, то адміністратор хосту мережі позбавлений такої можливості;

- невідома траєкторія доступу. Користувач або зловмисник може запросити доступ до ресурсів деякого вузла мережі, з яким цей вузол безпосередньо не пов'язаний.

У таких випадках доступ здійснюється через якийсь проміжний вузол, підключений до обох вузлів, або навіть через кілька проміжних вузлів. У мережевому середовищі непросто точно визначити, звідки надійшов запит на доступ, особливо якщо зловмисник докладає всіх зусиль, щоб приховати його;

- слабка захищеність лінії зв'язку. Мережа відрізняється від окремої системи тим, що вона, безумовно, включає лінії зв'язку, по яких передаються дані між вузлами.

Це може бути елементарний провід, а може бути лінія радіозв'язку, включаючи супутниковий канал. За певних умов (і відповідного обладнання) можна непомітно (або майже непомітно) підключитися до проводу, можна

успішно прослухати радіозв’язок – тобто ніщо не заважає «викачувати» передані повідомлення з ліній зв’язку і потім ізоляції необхідного.

На основі аналізу загроз безпеці комп’ютерної мережі можна зробити висновки про властивості та функції, якими повинна володіти система безпеки корпоративної мережі (КМ).

Ідентифікація захищених ресурсів, тобто присвоєння ідентифікаторів захищеним ресурсам - унікальні ознаки, за якими в подальшому система виконує аутентифікацію. Автентифікація захищених ресурсів, тобто їх ідентифікація на основі порівняння з еталонними ідентифікаторами. Застосувати парольний захист ресурсів. Розмежування доступу користувачів до КМ. Розмежування доступу користувачів за операціями (читання, запис, модифікація тощо) над ресурсами (програмами, файлами, каталогами, дисками, серверами тощо) за допомогою засобів адміністрування програмного забезпечення.

Реєстрація подій: вхід користувача в мережу, вихід з мережі, порушення прав доступу до захищених ресурсів тощо. Реакція на факти порушення прав доступу до захищених ресурсів мережі, несанкціоноване підключення до КМ. Забезпечення захисту інформації при проведенні робіт з обслуговування та ремонту.

3 ОЦІНКА РИЗИКІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Захист критичної інформаційної інфраструктури

Розвиток глобальних інформаційних систем створює широкі можливості як для розвитку різних галузей людської діяльності, так і для ускладнення та вдосконалення методів ведення кіберконфліктів (виведення з ладу критичних об'єктів) [1, 2]. У такому інформаційному просторі стрімко зростає кількість шкідливих програм і атак на комп'ютерні мережі. Антивіруси та брандмауери справляються з переважною більшістю з них, але деякі атаки можуть обійти такий захист, завдаючи шкоди користувачу чи компанії. Найчастіше існуючий захист спрацьовує із затримкою, коли система вже була атакована і сталася втрата даних або контролю над певними компонентами мережі [3, 4].

Захист критичної інформаційної інфраструктури є ключовою частиною захисту інформаційної безпеки. Основною метою захисту об'єктів критичної інфраструктури є зниження ризику втрати критичних даних та підвищення конфіденційності інформації [5]. Крім того, відповідний рівень захисту критичної інфраструктури дозволяє визначити найслабші вузли для зловмисного втручання в інформаційну систему або телекомунікаційну мережу для додаткового моніторингу та дослідження. Cross Technologies, залежно від їх застосування, дозволяють організувати багатофакторні системи та захист даних за допомогою взаємного спостереження та пошуку аномалій у діях мережі чи користувача [6].

Ключові елементи захисту критичної інформаційної інфраструктури включають:

1. Збір інформації про бізнес-процеси замовника.
2. Категоризація об'єктів обслуговування інформаційних систем, виділення важливих процесів.

3. Моделювання ситуацій, що загрожують інформаційним системам, мережам і системам управління. Визначення напрямків атаки на важливі об'єкти інформаційної системи.

4. Розробка та узгодження загальних вимог до рівня захисту інформації.

5. Розробка технічного проекту та комплекту робочої документації.

6. Оновлення існуючого захисту або виконання налагоджувальних робіт при створенні нової лінії захисту інформаційних систем.

7. Розробка методів тестування.

Найдосконаліші структури безпеки здебільшого керуються комерційними, а не державними компаніями. При цьому для підвищення безпеки навіть державним структурам потрібно максимально взаємодіяти (передати охорону критичних об’єктів) або переймати передовий досвід приватних фірм. Приватні компанії мають порівняно кращі показники, ніж державні, оскільки вільна конкуренція змушує їх постійно контролювати якість своєї продукції.

У деяких країнах запроваджено протоколи обміну інформацією та даними, щоб розподілити роботу з підтримки безпеки між відповідними структурами. Таке розповсюдження дозволяє своєчасно інформувати необхідні відділи про надходження важливих оновлень або наявність загрози. Також покращується координація дій, що сприяє ефективному використанню ресурсів.

Ця модель реалізована в Німеччині, де на державному рівні функціонують механізми розподілу важливих даних, які є основою для побудови систем захисту важливих інфраструктурних об’єктів. На основі цієї технології побудовано взаємодію між поліцією та спецслужбами через відповідні інформаційні центри, які дозволяють уніфікувати та передавати необхідну інформацію до необхідних органів [7]. Цей обмін побудований тільки між державними відомствами, але також налагоджено взаємодію з приватними компаніями для налагодження обміну досвідом у боротьбі з

вторгненнями (дозволяє обмінюватися лише некритичними даними про роботу державних мереж). Обмін інформацією відбувається через UP KRITIS та Alliance for Cyber Security [8]. Перша компанія відповідає за безпеку в області захисту критичної інформаційної інфраструктури між приватними та державними структурами, зосереджуючись на роботі критичних секторів. Alliance for Cyber Security відповідає за сферу комп'ютерної безпеки. Для взаємозв'язку компаній проводяться наради щодо поточних вторгнень у комп'ютерні мережі [9–14].

3.2 Аналіз ризиків

Оцінка ризику допомагає визначити можливі вторгнення, їх наслідки та ймовірність [15]. Аналіз ризиків є важливою частиною антикризового менеджменту. Залежно від масштабів діяльності компанії, оцінка ризиків може проводитися як самостійно, так і із залученням приватних компаній, які спеціалізуються на роботі з критичними інфраструктурами.

Типовим прикладом урядової оцінки ризиків є Швеція, де використовується алгоритм, який ідентифікував 27 серйозних вторгнень і розробив 11 сценаріїв протидії виникаючим ризикам.

Данія не дотримується національного плану оцінки ризиків, що дозволяє її департаментам самостійно керувати безпекою, а для взаємозв'язку між департаментами було створено Відділ оцінки кіберзагроз, за допомогою якого здійснюється комунікація та обговорення планів боротьби з вторгненнями та оцінки ризиків для різних галузей промисловості. відбуватися.

Швейцарія є прикладом децентралізованого управління ризиками. Швейцарія використовує підхід, який приділяє велику увагу індивідуальній

відповідальності. Підсектори самостійно керують виявленням вторгнень і атак. Вважається, що підгалузі найкраще знають, як працюють їхні системи.

Боротьба з кризами інформаційної безпеки полягає у розподілі відповідальності за кожним вузлом мережі. Алгоритми координації та прийняття рішень дозволяють узагальнити досвід, отриманий одним вузлом, на всю ієрархію. Кризове управління повинно бути скоординовано з усіма елементами мережі антикризового управління [16].

Прикладом добре структурованого менеджменту такого типу є Нідерланди, де застосовується Національний посібник із прийняття рішень у кризових ситуаціях. При такому підході у разі вторгнення контроль за ситуацією передається Національному координатору з питань безпеки та протидії тероризму, тому до вирішення проблеми залучаються кваліфіковані фахівці, які можуть швидко придушити небажану активність. Така структура дозволяє накопичувати максимум інформації про вторгнення в одному відділі, що дає можливість правильно реагувати на будь-які інциденти, що виникають.

Для успішної протидії кризам рекомендується співпрацювати з аутсорсинговими компаніями, тоді під час вторгнення її вирішенням займається спеціально створений відділ (Бюро швидкого реагування). Це Бюро створено як державно-приватне партнерство, яке надає консультації щодо обробки вторгнень. Таким чином, охорона організовується з урахуванням усіх особливостей функціонування даної системи.

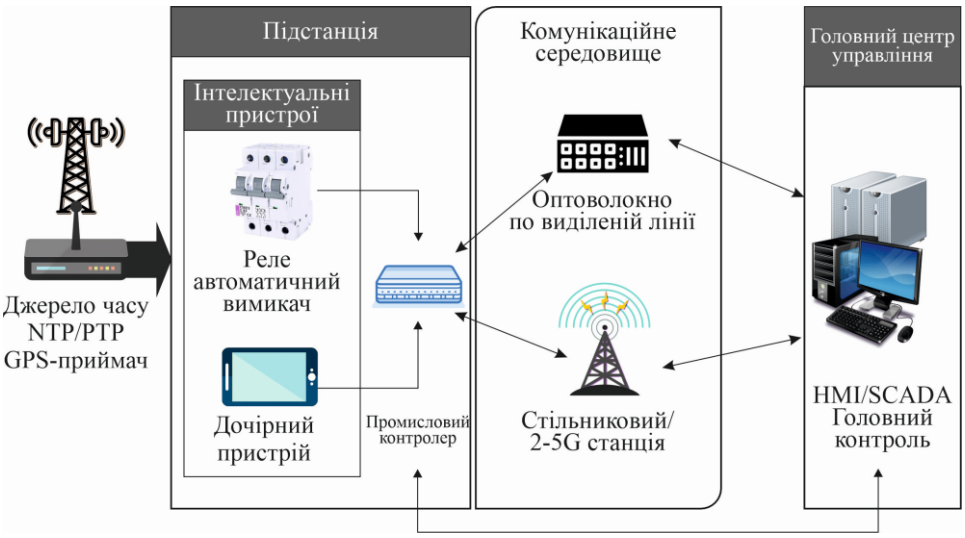

Рисунок 3.1 – Функціональна архітектура для сценарію атаки

На рис. 3.1 показано функціональну архітектуру, на якій базується більшість атак. Також потенційні ризики залежать від типу систем та їх реалізації. Залежність електроенергетики від телекомунікацій різна в залежності від використовуваних технологій, залучених суб'єктів і налаштувань пристроїв, включених в систему [17].

Зв'язок між електростанцією і центром управління може бути одностороннім і двостороннім. Односторонній зв’язок зазвичай передбачає отримання даних із системи SCADA, тоді як двосторонній зв’язок додатково передбачає надсилання команд назад. Промислові контролери часто використовуються як проміжне програмне забезпечення для уніфікації протоколів пристроїв і команд, що передаються. Це означає, що потенційні зловмисники також повинні скомпрометувати програмне забезпечення та системи контролера, перш ніж можна буде контролювати будь-які підстанції.

Програми для підстанцій включають візуалізацію та моделювання розподілених систем живлення, модальне балансування потужності та аналіз виробництва, аналіз після подій, який може запускати функцію реле відключення, перевірки часу для підстанцій та аналіз потоку. Одним із найпоширеніших і часто використовуваних інструментів є порогові вимірювачі нормальної та ненормальної активності користувача та продуктивності системи [11, 12, 18].

Особливості вторгнень на критичні об'єкти:

– Труднощі із забезпеченням захисту взаємопов’язаних об’єктів критичної інфраструктури.

– Труднощі із забезпеченням захисту вузлів мережі, які не підзвітні одному командному центру.

– За деякими характеристиками приватні компанії з інформаційної безпеки можуть перевершувати та швидше реагувати на загрози, ніж державні.

– У зв'язку зі швидким розвитком систем безпеки зростає кількість і складність нових видів атак.

– Складність оцінки можливої шкоди всій системі, коли вузли мережі виходять з ладу.

– Недосконаліть правового регулювання інформаційної війни не завжди може кваліфікувати атаку на критичні об'єкти як зловмисницьку.

На цьому етапі користувач має слабкий захист, який забезпечує більшість антивірусних компаній, оскільки він часто не є своєчасним (спочатку вірус поширюється, а вже потім антивіруси займаються його знищенням), чого достатньо для доступу зловмисника. необхідну інформацію або пошкодити наявну. Саме своєчасне сповіщення системи та користувача допоможе підвищити ефективність виявлення вторгнень як локально, так і в Інтернеті. При плануванні захисту важливо розрахувати ступінь захисту кожного вузла мережі, що дозволить визначити можливі шляхи атаки зловмисника і побудувати ефективний захист.

У Сполучених Штатах безпека критично важливих об’єктів, які складають критичну інфраструктуру, добре розвинена і включає:

– Системи сільськогосподарського та продовольчого забезпечення.

– Фінансово-банківська система.

– Транспортна система.

– Система водопостачання.

– Служби порятунку та швидкої допомоги.

– Система живлення.

– Система державного управління.

У США прийнято підрозділяти критичні об'єкти на об'єкти інфраструктури, пов'язані з міжнародними організаціями (об'єкти енергетики, транспорту, банківської справи, фінансової системи, зв'язку) і не пов'язані (водопостачання, служби порятунку, уряд). На основі аналізу поглядів керівництва США виділено три категорії критичних об’єктів:

Життєво важливі:

– Атомна станція.

– ГЕС (понад 2 ГВт).

– Гідротехнічні споруди.

– Сховища стратегічних запасів нафти і газу.

– Шкідливі хімікати та нафтохімія.

– Склади для зберігання ядерних матеріалів та боєприпасів.

Надзвичайно важливі:

– Системи електропостачання (більше 2 ГВт).

– Метро.

– Лінії водопостачання.

– Підземні каналізаційні системи.

– Магістральні трубопроводи.

Важливі:

– Морські порти.

– Очисні споруди.

– Магістральні споруди (в США близько 7 млн. км доріг, з них понад 80 тис. магістралей, понад 600 тис. мостів. Протяжність залізниць близько 550 тис. км.).

– Великі аеропорти (понад 500 великих аеропортів і більше 14 000 малих аеропортів і місць.

– Великі комунікаційні центри».

– Магістральні трубопроводи.

Існує 6 основних категорій впливу:

– Знищення або пошкодження.
– Економічний.
– Шкода навколишньому середовищу.
– Пошкодження національній обороні.
– Символічні.
– Другорядні проблеми національної безпеки.

Кожен сценарій вторгнення оцінюється за п'ятибальною шкалою загрози. При такому підході стає можливим неправильний розрахунок ризиків, пов’язаних з кожним видом загрози, що дозволить ефективно розподілити обчислювальні ресурси при плануванні захисту вузлів мережі. Наприклад, якщо вторгнення можливе з імовірністю 0,5 (50/50), можна визначити, що ймовірність використання конкретної атаки (наприклад, атаки Synflood на комп’ютерну мережу) становить 75/25 — ймовірність 0,75, то успішність такої атаки оцінюється як успішна 70/30, тобто ймовірність 0,3. Критерієм успішної атаки може бути вихід з ладу 25 вузлів мережі та фінансові втрати до 15 мільйонів євро. Цей ризик оцінюється за формулою:

$$L_{\text{tot}} = \left(L_{\text{hum}} + L_{\text{res}}\right) P_a P_t P_s, \tag{3.1}$$

де L_{tot} – загальний збиток; L_{hum} – людські втрати; L_{res} – втрата ресурсів; P_a – ймовірність нападу; P_t – ймовірність певного типу атаки; P_s – це ймовірність успішної атаки.

З наведених вище даних можна зробити висновок, що потенційний збиток становитиме вихід з ладу 2,8 вузлів мережі та економічний збиток у 1,68 млн. євро.

Для багатьох вторгнень у критичні системи можна використовувати спрощену систему оцінки небезпеки, наприклад, максимальний рівень загрози, середній або мінімальний. У цих категоріях загрози буде легше класифікувати та впоратися з ними.

Наведена вище оцінка ризиків добре підходить для багатовекторного аналізу можливих сценаріїв атак на ключові вузли критичних систем для виявлення найслабших або менш надійних елементів мережі. Також цей спосіб хороший для побудови ієрархії елементів мережі, вихід з ладу яких може спричинити за собою найбільші фінансові втрати (що особливо важливо для банківських структур, перебої в роботі яких тягнуть за собою не тільки втрату грошей, але і клієнтів). Цей підхід також застосовний для пошуку ефективних рішень для стримування повітряного руху [19].

Також важливо не допустити перевищення порогових значень кризового діапазону для критичного об’єкта.

Вміючи розрахувати ризик, стає можливим оцінити ефективність захисту, яку можна зробити на основі аналізу відповідних ризиків і шансів. На основі цього підходу можливі два види оцінок. Перший — це оцінка миттєвих значень, при яких змінна стану набуває певного значення.

Друга – інтегральна оцінка, коли змінна стану належить до певного діапазону значень. Інтегральна оцінка стану має кілька обмежень, пов’язаних головним чином із необхідністю узгодження результату з певним діапазоном попередньо визначених даних, що не завжди можливо реалізувати. Основні труднощі можуть виникнути при розрахунку можливих результатів і адекватності ймовірних реакцій на них (машинне навчання тут непридатне, оскільки збережеться загроза неадекватної реакції на загрозу або її пропуску, що неприйнятно для критичних систем). Тому найбільш прийнятною для оцінки ефективності захисту буде оцінка миттєвих значень, при яких змінна стану набуває певного значення. Ці оцінки певною мірою матимуть прогнозний характер. Такий підхід часто використовується при статистичному розрахунку можливих ризиків при роботі замкнутих автоматизованих систем [20, 21].

У цьому випадку необхідно оцінити очікувану ефективність, виходячи зі співвідношення випадковості та ризику:

$$E_f\left(x_i\right)=\frac{\text{Chance}\left(x_i\right)}{\text{Risk}\left(x_i\right)}=\frac{v\left(x_i\right)\left[1-F\left(x_i\right)\right]}{u\left(x_i\right)\Delta x f\left(x_i\right)}, \tag{3.2}$$

де x_i – значення граничного порогового стану на інтервалі $\left(x_l, x_m\right)$;

$$v\left(x_i\right)=x_l\left(\frac{x_i}{x_l}-1\right)-\lambda\left(\frac{x_i}{x_l}-1\right)^2$$

пошкоджується при перевищенні граничних значень точки x_i, кризового інтервалу $\left(x_l, x_m\right)$;

$$u\left(x_i\right)=\lambda\left(\frac{x_i}{x_l}-1\right)$$

очікувана вигода від досягнення екстремальних значень x_i, кризового інтервалу $\left(x_l, x_m\right)$; x_l, x_m – це пороги безпеки, в межах яких оцінюються шанси та ризики; μ і β – параметри положення та форми кривої розподілу.

Таким чином, ККД на момент досягнення критичного значення x_i становитиме:

$$E_f\left(x_i\right)=\frac{\underline{v}\left(x_i\right)\left[1-F\left(x_i\right)\right]}{\underline{u}\left(x_i\right)\Delta x f\left(x_i\right)}=\frac{\beta\left(1-\mathrm{e}^{-\mathrm{e}^{\frac{\mu-x_i}{\beta}}}\right)\underline{v}\left(x_i\right)}{\mathrm{e}^{\frac{\mu-x_i}{\beta}-\mathrm{e}^{\frac{\mu-x_i}{\beta}}}\underline{u}\left(x_i\right)\Delta x}, \tag{3.3}$$

де Δx – критичний крок зміни стану

Розраховуючи таким чином ефективність, можна більш ефективно розподіляти обчислювальні ресурси під час побудови захисту для критичних

об’єктів. Процес прогнозування ефективності захисту важливого об’єкта, в контексті забезпечення захисту змінних стану, показано на рис. 3.2.

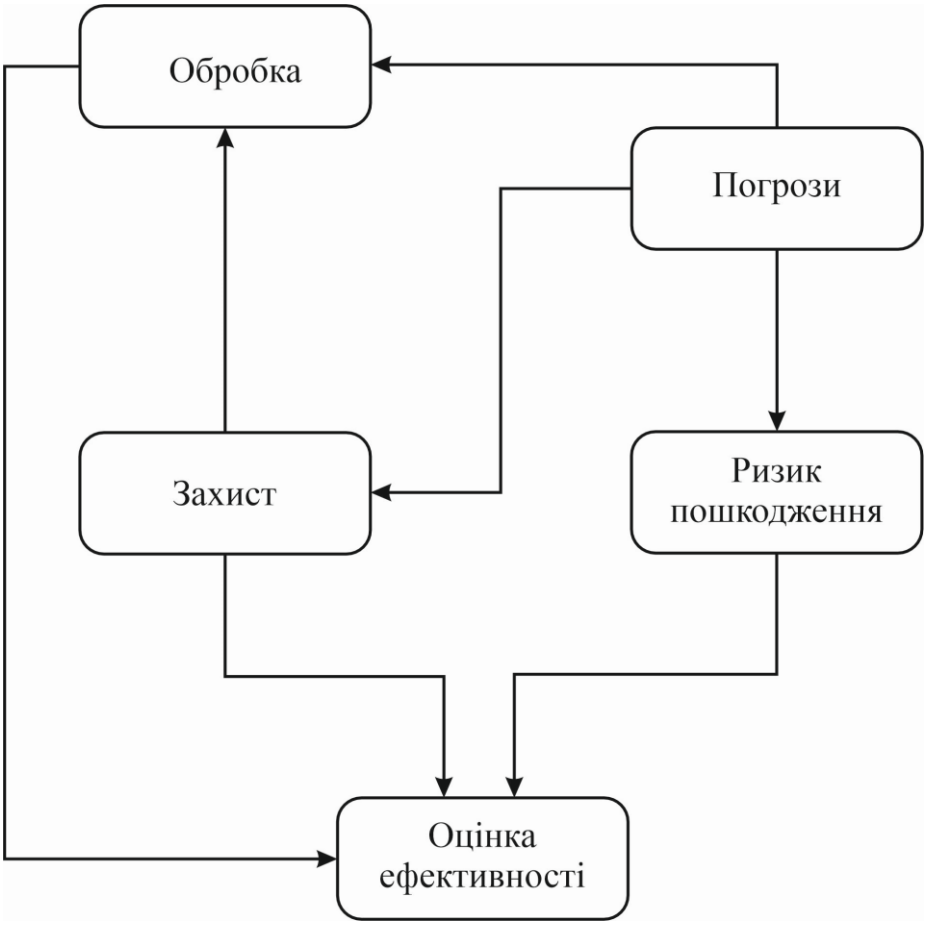

Рисунок 3.2 – Структура процесу забезпечення безпеки критичного об'єкта

Стабільність соціально-економічного розвитку країни та її безпека безпосередньо залежать від надійності та безпеки функціонування критичних об’єктів, тому вкрай важливо досліджувати можливі ризики, що виникають внаслідок непередбачуваних ситуацій чи атак зловмисників.

4 БЕЗПЕКА НА МЕЖІ МЕРЕЖІ: АРХІТЕКТУРА РОЗПОДІЛЕНОГО БРАНДМАУЕРА

4.1 Залежне від топології управління

Нові технологічні тенденції, такі як мобільні обчислення, обчислення між компаніями та клієнтські VPN, змушують адміністраторів безпеки переглянути спосіб захисту своїх мереж. Ці тенденції напружують існуючу інфраструктуру безпеки та виявляють властиві недоліки поточної технології брандмауера. Експерти з галузі безпеки, обговорюючи ці тенденції на семінарі High Assurance Boundary Controller, дійшли висновку, що забезпечення безпеки мережі має бути ближче до хосту. Це означає, що потрібно ще більше брандмауерів, в ідеалі один брандмауер для кожного хоста.

Сучасні мережеві інженери та адміністратори безпеки скуті в гонці з рішучими зловмисниками. Дві команди намагаються працювати разом, але вони фактично стримують одна одну. Мережні інженери забезпечують маршрутизацію трафіку, високу доступність і високу пропускну здатність. Вони роблять це частково, вирішуючи, де в топології створювати зв’язки та встановлювати маршрутизатори, брандмауери тощо. Адміністратори безпеки гарантують, що лише потрібним користувачам надається доступ до різноманітних доступних мережевих ресурсів. Вони роблять це, вирішуючи, де в топології мережі встановити брандмауери/фільтруючі маршрутизатори та які правила фільтрації мають бути реалізовані в кожному з цих проміжних мережевих пристроїв. Будь-яка зміна в одній сфері впливає на іншу. Комп'ютерні вчені визнають це проблемою зв'язку та когезії

Наступні нові технологічні тенденції виявляють додаткові недоліки в управлінні політикою, що залежить від топології:

VPN клієнт-сервер. VPN є важливим інструментом для захисту наших мереж. Ранні VPN часто реалізовувалися між парою шлюзів. Ці шлюзи

зазвичай були маршрутизаторами або міжмережевими екранами. Однак VPN-клієнти широко розгортаються, і кожна копія Windows 2000 постачається з вбудованою функцією VPN. Логічним результатом є те, що незабаром ми побачимо широке використання клієнт-серверних VPN. Це палиця з двома кінцями. Ці клієнт-серверні мережі VPN засліплюють противників, які можуть винюхати дані з мережі. Однак вони також закривають проміжні пристрої безпеки мережі, такі як брандмауери та маршрутизатори, які раніше могли фільтрувати такий трафік.

Коаліція та бізнес-партнери. Інформація цінна, якщо ви можете поділитися нею з потрібними людьми в потрібний час. Щоб досягти цього, Міністерство оборони та комерційний світ відкривають свої мережі для партнерів по коаліції чи ділових партнерів. Надання партнерам обмеженого доступу до певних систем у вашій мережі часто є єдиним практичним способом дозволити їм отримати потрібну інформацію вчасно. Адміністратори безпеки повинні підтримувати цей новий спосіб ведення бізнесу. Однак це складно, оскільки дозвіл партнерам глибоко проникати в наші мережі стирає відмінність між інсайдерами та аутсайдерами. Стара парадигма периметрального брандмауера, «припустимо, що всі всередині брандмауера є хорошими інсайдерами, а всі поза брандмауером є підозрілими», більше не працює.

Мобільні обчислення. Багато наших засобів захисту мережі передбачають стаціонарні обчислення. Тобто конкретний клієнт або сервер фізично підключений до топології мережі у фіксованій точці. Це дозволяє розміщувати проміжні мережеві пристрої (фільтруючі маршрутизатори та брандмауери) у стратегічних точках топології для контролю потоків між парою хостів. Цю стару парадигму кидає виклик впровадження мобільних і бездротових обчислень. Сьогодні користувач з ноутбуком очікує підключитися до мережі організації, незалежно від того, в якій будівлі він знаходиться, і отримати доступ до систем, до яких він має доступ.

Простий приклад на рис. 4.1 ілюструє проблеми, коли мобільні обчислення використовуються в організації, яка використовує топологічно залежне управління політикою. У прикладі організації є дві групи, які іноді працюють разом, але жодна група не дозволяє користувачам за межами своєї групи отримувати доступ до серверів рівня групи. Зокрема, користувач Joe має авторизований доступ до синіх серверів, але він не має авторизованого доступу до зелених серверів. Організація реалізує цю політику за допомогою фільтрів пакетів у маршрутизаторах 1 і 2. Маршрутизатор 1 реалізує правила фільтрації пакетів, які блокують будь-який трафік до/з зеленої підмережі. Маршрутизатор 2 реалізує фільтри пакетів, які блокують будь-який трафік до/з синьої підмережі.

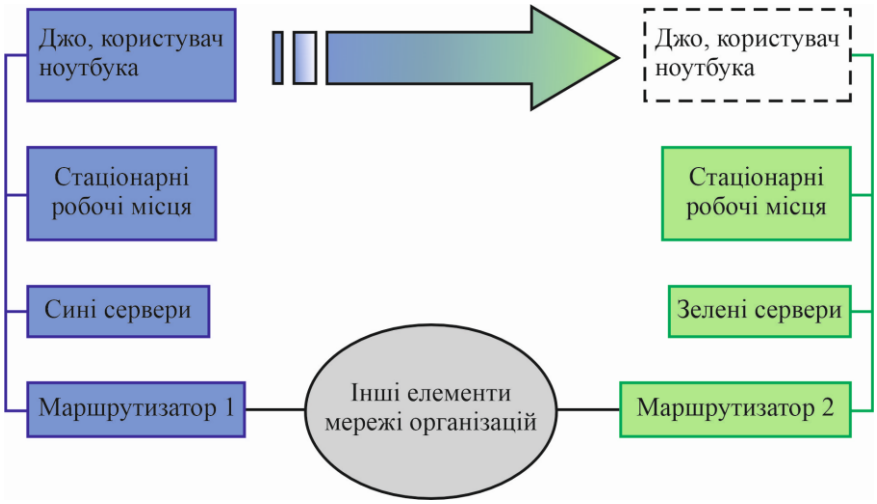

Рисунок 4.1 – Мобільні комп’ютери підривають традиційну безпеку мережі.

Усе працює добре, поки Джо не відкриває потужність і ефективність ноутбуків. Джо доручено взяти участь у нараді в офісі зеленої групи. Джо бере з собою свій ноутбук і підключається до мережі в зеленій конференц-залі. Джо розчарований (і неефективний), оскільки він не може отримати доступ до синіх серверів, до яких він має доступ, щоб представляти синю групу на зустрічі. Джо повинен повернутися до синьої будівлі, щоб відповісти на запитання, поставлені під час зустрічі.

Безпека на основі топології не тільки запобігає доступ мобільного користувача Джо до авторизованих ресурсів. Він також не може заблокувати

загрозу несанкціонованого доступу. Коли Джо підключено до зеленої мережі, він міг:

1. Запустити сніфер мережі на його ноутбуці та захопити ім’я користувача/паролі до зелених серверів.
2. Використати ці захоплені паролі, щоб отримати неавторизований доступ до зелених серверів.

Безпека, реалізована в проміжних мережевих пристроях і залежить від топології мережі, з тріском провалюється в мобільному комп’ютерному середовищі.

Навіщо використовувати бездротові обчислення, якщо користувачі не можуть підключитися до мережі в будь-якій точці під час роумінгу? Технологія безпеки повинна підтримувати мобільні машини, які сьогодні перебувають усередині брандмауера, а завтра – за його межами. Або в підмережі X сьогодні та підмережі Y завтра.

4.2 Незалежне від топології управління

Ключ до перемоги в гонці безпеки полягає в тому, щоб від’єднати мережевих інженерів від адміністраторів безпеки. Оскільки топологія мережі – це шнур, який зв’язує, ми повинні відокремити топологію мережі від застосування політики безпеки, прийнявши перспективу кінцевої точки для керування безпекою.

Network Edge Security відокремлює адміністраторів безпеки від мережевих інженерів, переміщуючи PEP (точки застосування політики) за межі ядра мережі та розміщуючи їх на межі мережі. Тоді PEP прив’язуються до хостів, а не до топології мережі. Це значно спрощує адміністрування безпеки. Наприклад, розглянемо організацію з політикою безпеки.

• Жодна машина не авторизована для аналізу трафіку (наприклад, паролів) з мережі

• Жодній машині не дозволено надсилати пакети з підробленими IP-адресами

• Права доступу.

Ця тривіальна політика стає нетривіальною для реалізації за допомогою проміжних мережевих пристроїв у простій топології, показаній на рис. 4.2. Процес реалізації політики, що залежить від топології, зазвичай включає наступні 3 кроки.

1. Вказати політику клієнт-сервер.

2. Проаналізувати топологію мережі, включаючи розташування клієнтів, серверів і проміжних мережевих пристроїв (маршрутизатори фільтрації та брандмауери). Передбачити також мобільні комп'ютери (наприклад, ноутбуки відділу продажів), які можуть підключатися до мережі в кількох точках.

3. Створити список ACL і правило фільтрації для кожного проміжного мережевого пристрою на шляху між кожним клієнтом і кожним сервером.

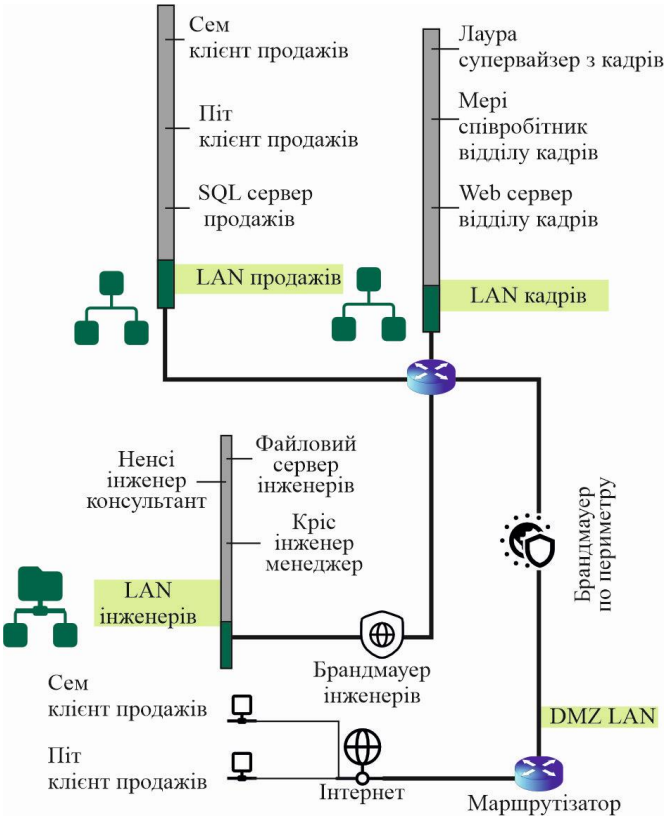

Рисунок 4.2 – Проста топологія для прикладу політики

Зауважимо, що деякі частини політики, такі як заборона перехоплення та керування в сегменті локальної мережі, не можуть застосовуватися існуючими маршрутизаторами та брандмауерами. Тепер опишемо потрібну політику, використовуючи топологічно незалежне керування політикою, як показано на рис. 4.3. Процес впровадження зазвичай включає наступні два кроки.

1. Укажіть політику клієнт-сервер (наприклад, таблиця 1).
2. Створіть правила фільтрації для кожної групи публічних діячів безпосередньо з таблиці правил. Усі PEP налаштовані на відсутність шпигування та спуфінгу.

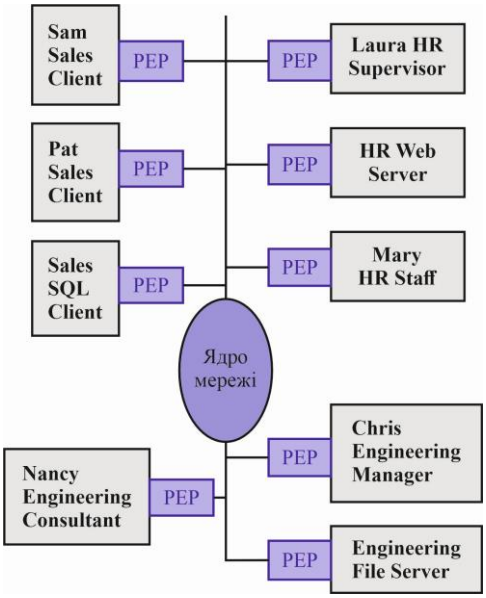

Рисунок 4.3 - Застосування безпеки незалежно від топології

Незалежне від топології забезпечення безпеки розв’язує руки адміністратора безпеки та мережевого інженера. Однак це відкриває питання щодо безпеки та масштабованості. Тепер адміністратори керують відносно великою кількістю простих політик на відміну від складних політик, які керуються брандмауерам периметра. Для кожного мережевого адаптера можна створити унікальну політику. Проте більшість організацій можуть значно зменшити ризик, спільним використанням політик між групами машин, що використовуються для подібних завдань. Безпеку можна значно підвищити майже з нульовим адміністративним навантаженням, просто

призначивши кожному мережевому адаптеру загальну політику «хорошої гігієни», яка блокує перехоплення паролів і підробку адрес.

4.3 Архітектура безпеки краю мережі

Network Edge Security — це архітектура брандмауера другого покоління, яка змінює парадигми брандмауера першого покоління. Уявіть, що ви намагаєтеся захистити свій дім від несанкціонованого доступу, встановивши поліцейський контрольно-пропускний пункт на міжштатній трасі поблизу вашого дому. Звичайно, це було б безглуздо. Однак багато організацій намагаються захистити свої хости від несанкціонованого доступу, встановлюючи брандмауери 1-го покоління на основних мережевих маршрутах.

Представимо архітектуру Network Edge Security і покажемо, як вона змінює парадигми адміністрування політики. Також вкажемо на такі архітектурні особливості, як можливість обходу, захист від несанкціонованого доступу та масштабованість. Команда Autonomic Distributed Firewall реалізувала PEP за допомогою комерційних мережевих інтерфейсних карт Ethernet (NIC). З цього моменту стаття зосереджується на NIC як на одному екземплярі абстрактного PEP.

На рис. 4.4 показана архітектура системи. Архітектура головний/підлеглий забезпечує централізоване керування розподіленими точками виконання. Сервер політики забезпечує всі функції інтерфейсу користувача, керування політикою, керування групою NIC (PEP) і функції аудиту бази даних. Сервер політики створює політику та надсилає її до мережевих карток. Мережні карти забезпечують фільтрацію пакетів та інші прості функції підтримки безпеки мережі. Цей підхід розміщує складні

функції на сервері політики, що дозволяє мережевим картам бути простими, швидкими та недорогими.

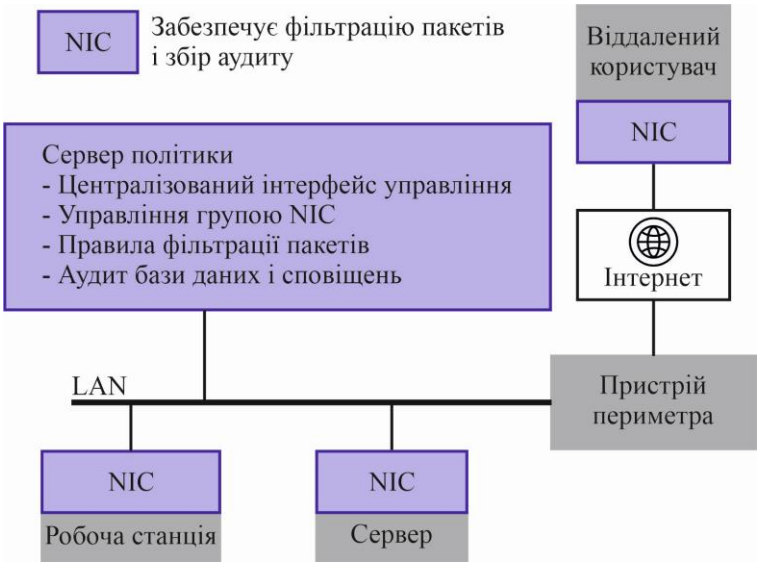

Рисунок 4.4 – Архітектура системи Network Edge Security

Деякі представники спільноти безпеки визнали цінність перенесення функції брандмауера ближче до хоста. У результаті зростає список комерційно доступних програмних брандмауерів або персональних брандмауерів. Використання цих брандмауерів в організаційному середовищі викликає серйозні питання щодо їх стійкості до несанкціонованого доступу.

Чому вперше були побудовані брандмауери? Оскільки комерційні операційні системи та програми неодноразово демонстрували, що їх надзвичайно важко захистити. Програми стали складнішими після появи брандмауерів. Поточними загрозами є Active-X, JavaScript і віруси/хробаки, що передаються електронною поштою. Операційні системи також стали складнішими, оскільки до них додається все більше функцій. Чистий ефект полягає в тому, що організації CERT не скорочують свій штат. Що відбувається, коли в це середовище вводять програмні брандмауери на основі хоста? Не дивно, що вони не відповідають фундаментальній вимозі захисту від несанкціонованого доступу.

Програма DARPA Information Assurance перевірила один із цих програмних брандмауерів. Брандмауер було встановлено на робочій станції, і червона команда Sandia почала атакувати його з усієї мережі. Брандмауер блокував прості атаки, такі як сканування портів. Потім червона команда створила повідомлення електронної пошти з вбудованим сценарієм. Це повідомлення було надіслано на робочу станцію, захищену програмним брандмауером. Коли мимовільний користувач відкрив електронний лист, сценарій виконувався з усіма привілеями користувача. Сценарій повністю вимкнув брандмауер, але залишив значок брандмауера на екрані. Політику брандмауера було повністю порушено, і користувач залишився з помилковим відчуттям безпеки.

За іронією долі ці програмні брандмауери були відключені іншим програмним забезпеченням безпеки. Антивірусне програмне забезпечення Symantec помилково визначило брандмауер BlackICE Network ICE як троянського коня. Результат: антивірусне програмне забезпечення вимкнуло брандмауер і залишило багато ПК домашніх користувачів уразливими. [4] Ці випадки відключення програмних брандмауерів не повинні бути несподіванкою. Існує циклічна логіка, що лежить в основі архітектури програмних брандмауерів на основі хосту, яку не можуть виправити розробники, які пишуть код. Рис. 4.5 ілюструє цю циклічну логіку. Постачальники безпеки розробляють брандмауери для захисту головної операційної системи. Однак ці програмні брандмауери на основі хоста покладаються на операційну систему хоста для захисту брандмауера. Брандмауер захищає операційну систему чи операційна система захищає брандмауер? Ситуація ще гірша, якщо ворожий користувач контролює машину.

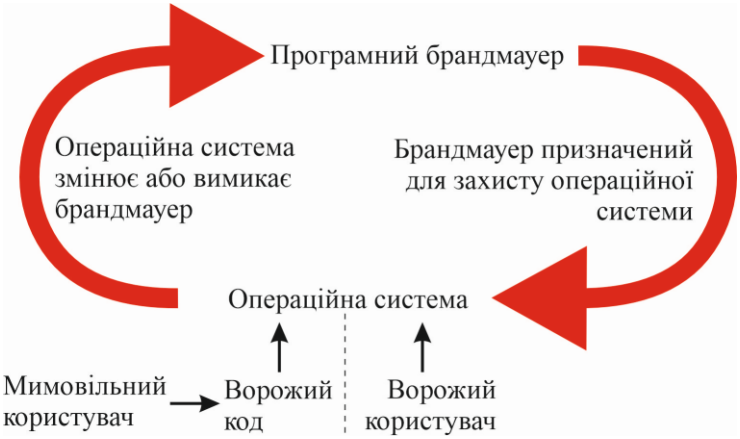

Рисунок 4.5 – Програмні брандмауери на основі хостів страждають від циклічної логіки

Суть полягає в тому, що хоча програмні брандмауери на основі хосту пропонують певний захист для домашнього користувача, вони не відповідають вимогам організації, яка піклується про безпеку. Персональні брандмауери були створені в основному для захисту хоста від мережі. Network Edge Security було створено, щоб захистити мережу організації від підривного хоста та ворожих інсайдерів.

Network Edge Security реалізовано як віддалено керований пристрій для застосування політики, який не залежить (з точки зору застосування політики) від операційної системи хоста. Network Edge Security NIC містить власний процесор і пам’ять, які недоступні операційній системі чи програмам. Навіть недоброзичливий користувач за клавіатурою з правами root/адміністратора не може змусити пристрій змінити політику, встановлену адміністратором. Мережевий адаптер може бути налаштований на надсилання періодичного сигналу на сервер політики, щоб зменшити загрозу непоміченого фізичного втручання. Суть полягає в тому, що мережевий адаптер Network Edge Security не можна обійти та захищений від несанкціонованого доступу.

Network Edge Security має масштабуватися, щоб відповідати потребам організацій реального світу. Управління, пропускна здатність і підтримувані платформи мають збільшуватися.

Це архітектура головний/підлеглий, а не архітектура клієнт/сервер. Ключова відмінність полягає в тому, що брандмауери для кожного хоста є підлеглими для менеджера вузлів. В архітектурі клієнт/сервер клієнти вимагають від сервера виконати функцію або надати дані. У архітектурі головний/підлеглий менеджер вузлів має абсолютні повноваження та надсилає команди політики на вузли брандмауера (NIC) для примусового виконання. Цей підхід до керування підтримує тисячі мережевих карток в організації.

Продуктивність підходу Network Edge Security легко масштабується. Щоразу, коли до мережі додається новий хост, до розподіленого брандмауера додається додатковий процесор NIC. Комерційна реалізація дозволяє використовувати декілька серверів політики, тому функція сервера політики також масштабується.

Брандмауери для кожного хоста є простими та незалежними від операційної системи хоста. Це дозволяє розгортати їх на різних хостах, типових для великих організацій. Мережні карти можуть захищати робочі станції та сервери в локальній мережі, а також віддалені хости.

Брандмауери першого покоління були розроблені в середовищі, в якому ризик з боку Інтернету вважався високим, а ризик від інсайдерів вважався низьким. Сьогодні зрозуміло, що внутрішня загроза коштує дорого, навіть якщо вона трапляється рідше, ніж атаки з Інтернету. Визначення інсайдерів розмивається через партнерства, які дозволяють отримати доступ до внутрішніх ресурсів користувачам, які не є членами організації. Мобільні комп’ютери також надають інсайдерам доступ до мереж, до яких вони не могли отримати доступ, коли їхній комп’ютер залишався на столі. Нарешті, ворожий код може перетворити лояльних інсайдерів на мимовільних агентів. Ці зміни в загрозах і ризиках змушують нас запитати, де оптимальне розташування брандмауерів.

Брандмауери по периметру, які відокремлюють організацію від Інтернету, сліпі для атак, запущених мимовільними інсайдерами та

ворожими інсайдерами. Ці брандмауери можуть забезпечувати певний захист від партнерів, які зловживають своїми правами доступу, якщо не використовуються VPN клієнт-сервер. Ці VPN ефективно закривають брандмауери по периметру.

Зрозуміло, що потрібно перенести функції брандмауера глибше в мережу організації. Внутрішні стіни, які розділяють групи всередині організації, є розумною спробою вирішити цю потребу. Однак вони страждають від наступних недоліків.

• Внутрішні стіни, як і брандмауери периметра, закриваються мережами VPN від клієнта до сервера.

• Внутрішні стіни не відповідають належним чином користувачам мобільних комп'ютерів, які можуть буквально переносити свій комп'ютер з одного боку стіни на іншу.

• Внутрішні стіни залежать від топології. Таким чином, вони ускладнюють керування політикою безпеки, прив'язуючи адміністраторів безпеки до мережевих інженерів.

• Внутрішні стіни нічого не запобігають проникненню паролів зловмисниками.

Ці проблеми дають зрозуміти, що функцію брандмауера потрібно перенести на окремі хости. Це може забезпечити необхідні функції брандмауера в потрібному місці, оскільки мобільні/бездротові обчислення та клієнтські серверні VPN стають поширеними.

Як запровадити брандмауер на кожному хості? Двома очевидними варіантами є брандмауери на основі програмного забезпечення та апаратні пристрої, незалежні від операційної системи.

Обмеження брандмауерів програмного забезпечення на основі хоста (таких як персональні брандмауери) обговорювалися вище. Програмних брандмауерів недостатньо, оскільки вони не можуть забезпечити захист від несанкціонованого доступу, необхідний для запобігання ворожим інсайдерам і мимовільним інсайдерам, які запускають ворожий код. У спробі перенести

функції брандмауера з периметра на хост ці реалізації програмного забезпечення пішли «через край». Нам потрібно відключити брандмауер від головної операційної системи.

Реалізація брандмауера має бути достатньо близькою до хоста, щоб його не можна було обійти, але незалежно від операційної системи хоста. Апаратна реалізація на мережевій картці з власним процесором і пам’яттю, до яких хост не може отримати доступ, відповідає вимогам захисту від несанкціонованого доступу.

Враховуючи те, що ми дійшли висновку, що апаратний брандмауер для кожного хоста є правильною архітектурою, як нам керувати всіма цими брандмауерам? Брандмауерами мають керувати окремі користувачі чи професіонали з інформаційних технологій, навчені мережевій безпеці? Окремі користувачі, які можуть бути лояльними до організації, як правило, не мають знань про мережеві технології, щоб правильно налаштувати брандмауер. Спрощені користувальницькі інтерфейси, які пропонують «низький, середній і високий» рівень безпеки, як правило, не враховують певні функції, пов’язані з користувачем/хостом. Наприклад

• Чи повинен користувач/хост мати авторизований доступ Telnet до серверів?

• Чи повинен користувач/хост мати необмежений доступ до інших робочих станцій в організації?

• Чи повинен користувач/хост мати доступ до всіх серверів чи лише до певної підмножини серверів?

Навіть найкращий користувальницький інтерфейс на основі хоста стає неактуальним у руках ворожого інсайдера. Природно, навчений персонал безпеки мережі, відповідальний за виконання політики, повинен налаштувати брандмауери.

Враховуючи, що персонал IT/ІБ повинен налаштовувати/запроваджувати політику, цей персонал вимагатиме централізованого/віддаленого керування. Сервер політики забезпечує централізовану специфікацію політики, розповсюдження та аудит. Тривають

дослідження та розробки , спрямовані на пошук шляхів підвищення можливостей керування системою. Це включає розширення системи для включення автентифікації користувачів та інших підходів для мінімізації адміністративного навантаження.

4.4 Застосування захисту периферійної мережі до серверів, які спільно використовуються партнерами

Мережні мережеві карти Network Edge Security забезпечують недорогий інструмент із високою надійністю, який можна застосувати інноваційними способами для створення безпечних мережевих рішень. Спільні сервери обговорюються як приклад.

Часто партнерам потрібно ділитися доступом до онлайн-даних. Переміщення даних між партнерами через «Sneaker net» надто повільне. Темпи та структура операцій сьогодні вимагають, щоб партнери мали змогу взаємодіяти з нашими даними, а не просто переглядати їх. Наприклад, постачальникам може знадобитися можливість оновлювати інформацію про доставку в базі даних логістики. Одним із методів забезпечення цієї можливості є надання партнерам доступу до наших серверів. Однак надання партнерам облікових записів на наших серверах, підключених до наших внутрішніх мереж, створює певні ризики. Що робити, якщо партнер зловживає своїми правами доступу та отримує доступ до інших машин у нашій мережі?

Network Edge Security дозволяє створювати спільні сервери між парою організацій з мінімальною довірою між ними. На рис. 4.6 показано, як реалізувати набір спільних серверів між партнерами в синіх і фіолетових організаціях.

Синя організація налаштовує свій внутрішній мережевий адаптер (NIC_BI) за такою політикою.

• Дозволяє трафік HTTP, SMTP і SQL, який ініціюється від синьої локальної мережі до сервера.

• Блокувати весь трафік, ініційований із спільного сервера до синьої локальної мережі

• Блокує сервер від перехоплення будь-якого трафіку, що надходить через синю локальну мережу

• Налаштовує зовнішній мережевий адаптер (NIC_BE) за такою ж політикою.

• Вимагає IPSEC VPN для NIC_PE

• Блокує всі інші з'єднання

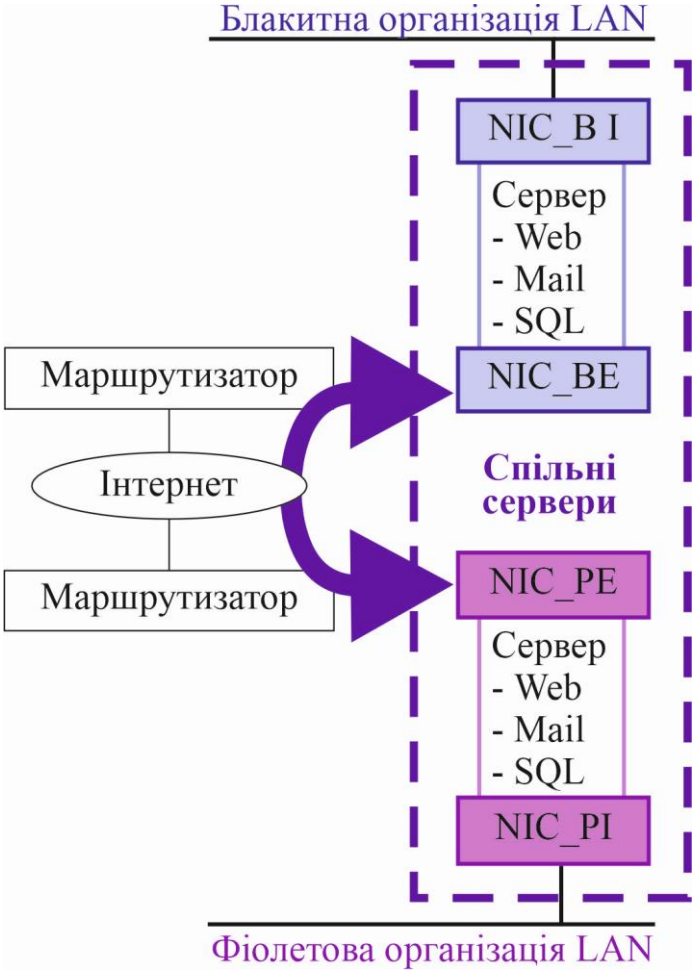

Рисунок 4.6 – Спільні сервери між парою партнерів

Фіолетова організація налаштовує свої мережеві карти з відповідною політикою, замінюючи «синій» на «фіолетовий». Це дозволяє кожній

організації ініціювати переміщення даних до та зі свого кінця спільного сервера. Фіолетова організація не може отримати доступ до синьої локальної мережі. Навіть якщо фіолетовій організації надано адміністраторський доступ до синього сервера, вони не можуть ініціювати трафік або перехоплювати трафік із синьої локальної мережі. VPN (товста стрілка) між серверами гарантує, що жодні суб'єкти в Інтернеті не зможуть переглядати або підробляти трафік між серверами. «Блокувати всі інші підключення» означає, що зовнішні мережеві карти підключаються один до одного, а не до інших машин.

Результатом є те, що кожна організація зберігає повний контроль над своєю власною локальною мережею без ризику того, що партнер може отримати несанкціонований доступ до локальної мережі. Кожна організація має живе мережеве підключення до свого кінця сервера. Таким чином, вони можуть публікувати в ньому дані, маніпулювати ними та читати їх у режимі реального часу. Це усуває проблеми зі старими даними, пов'язані з використанням sneaker-net для обміну інформацією. Партнер може отримати доступ лише до даних, розміщених на сервері відповідною хост-організацією. Таким чином, це набагато безпечніше, ніж фактично дозволити партнеру отримати доступ до ваших серверів, як це роблять деякі організації сьогодні.

ВИСНОВКИ

Представлено огляд і порівняння методів захисту критичних об’єктів для виявлення вразливих вузлів у системах, що використовуються.

Розглянуто основні засоби захисту критичних об'єктів та забезпечення їх працездатності під час надзвичайних ситуацій.

Визначено основні загрози безпеці інформації в лініях зв’язку комп’ютерних мереж та запропоновано методи розрахунку їх стійкості.

Запропоновано способи оцінки ефективності захисту, які можна здійснити на основі аналізу відповідних ризиків і шансів.

Встановлено, що програмні брандмауери не призначені для боротьби з внутрішньою загрозою.

Показано, що Network Edge Security являє собою апаратний брандмауер 2-го покоління, який усуває існуючу внутрішню загрозу та відповідає новим вимогам, а також поєднує топологічно незалежне управління політикою з високою безпекою та масштабованістю.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. A review paper on network security and cryptography / S. Tayal et al. *Advances in computational sciences and technology*. 2017. Vol. 10, no. 5. P. 763–770. URL: https://www.ripublication.com/acst17/acstv10n5_10.pdf.

2. Khan R. Network threats, attacks and security measures: a review. *International journal of advanced research in computer science*. 2017. Vol. 8, no. 8. P. 116–120. URL: https://doi.org/10.26483/ijarcs.v8i8.4641 (date of access: 26.01.2024).

3. Social network security: issues, challenges, threats, and solutions / S. Rathore et al. *Information sciences*. 2017. Vol. 421. P. 43–69. URL: https://doi.org/10.1016/j.ins.2017.08.063 (date of access: 26.01.2024).

4. Security threats in the data plane of software-defined networks / S. Gao et al. *IEEE network*. 2018. Vol. 32, no. 4. P. 108–113. URL: https://doi.org/10.1109/mnet.2018.1700283 (date of access: 26.01.2024).

5. Islam T., Manivannan D., Zeadally S. A classification and characterization of security threats in cloud computing. *International journal of next-generation computing*. 2016. Vol. 7, no. 1. P. 1–17. URL: https://doi.org/10.47164/ijngc.v7i1.101.

6. Virtual network security: threats, countermeasures, and challenges / L. R. Bays et al. *Journal of internet services and applications*. 2015. Vol. 6, no. 1. URL: https://doi.org/10.1186/s13174-014-0015-z (date of access: 26.01.2024).

7. Sinha P., Rai A. K., Bhushan B. Information Security threats and attacks with conceivable counteraction. *2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT)*, Kannur,Kerala, India, 5–6 July 2019. 2019. URL: https://doi.org/10.1109/icicict46008.2019.8993384 (date of access: 26.01.2024).

8. Dastres R., Soori M. Impact of meltdown and spectre on CPU manufacture security issues. *ResearchGate*. URL:

https://www.researchgate.net/publication/344604531_Impact_of_Meltdown_and_Spectre_on_CPU_Manufacture_Security_Issues.

9. Tayal A., Mishra N., Sharma S. Active monitoring & postmortem forensic analysis of network threats: a survey. *International journal of electronics and information engineering*. 2017. Vol. 6, no. 1. P. 49–59. URL: https://doi.org/10.6636/IJEIE.201703.6(1).05.

10. Review and evaluation of security threats on the communication networks in the smart grid / Z. Lu et al. *MILCOM 2010 - 2010 IEEE military communications conference*, San Jose, CA, USA, 31 October – 3 November 2010. 2010. URL: https://doi.org/10.1109/milcom.2010.5679551 (date of access: 26.01.2024).

11. Simmonds A., Sandilands P., van Ekert L. An ontology for network security attacks. *Lecture notes in computer science*. Berlin, Heidelberg, 2004. P. 317–323. URL: https://doi.org/10.1007/978-3-540-30176-9_41 (date of access: 26.01.2024).

12. Pawar M. V., Anuradha J. Network security and types of attacks in network. *Procedia computer science*. 2015. Vol. 48. P. 503–506. URL: https://doi.org/10.1016/j.procs.2015.04.126 (date of access: 26.01.2024).

13. Greitzer F. L., Hohimer R. E. Modeling human behavior to anticipate insider attacks. *Journal of strategic security*. 2011. Vol. 4, no. 2. P. 25–48. URL: https://doi.org/10.5038/1944-0472.4.2.2 (date of access: 26.01.2024).

14. Kaynar K. A taxonomy for attack graph generation and usage in network security. *Journal of information security and applications*. 2016. Vol. 29. P. 27–56. URL: https://doi.org/10.1016/j.jisa.2016.02.001 (date of access: 26.01.2024).

15. AutoSecSDNDemo: demonstration of automated end-to-end security in software-defined networks / R. Khondoker et al. *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, Seoul, South Korea, 6–10 June 2016. 2016. URL: https://doi.org/10.1109/netsoft.2016.7502404 (date of access: 26.01.2024).

16. Internet of things (IoT) security: current status, challenges and prospective measures / R. Mahmoud et al. *2015 10th international conference for internet technology and secured transactions (ICITST)*, London, United Kingdom, 14–16 December 2015. 2015. URL: https://doi.org/10.1109/icitst.2015.7412116 (date of access: 26.01.2024).

17. Design of secure user authenticated key management protocol for generic iot networks / M. Wazid et al. *IEEE internet of things journal*. 2018. Vol. 5, no. 1. P. 269–282. URL: https://doi.org/10.1109/jiot.2017.2780232 (date of access: 26.01.2024).

18. Kobo H. I., Abu-Mahfouz A. M., Hancke G. P. A survey on software-defined wireless sensor networks: challenges and design requirements. *IEEE access*. 2017. Vol. 5. P. 1872–1899. URL: https://doi.org/10.1109/access.2017.2666200 (date of access: 26.01.2024).

19. Stawowski M. The principles of network security design. *Advanced Cyber Solutions*. URL: http://advancedcybersolutions.com/HTML/Articles/PrinciplesNetworkSecurityDesign.pdf (date of access: 26.01.2024).

20. Barrera D., Molloy I., Huang H. Standardizing iot network security policy enforcement. *Workshop on decentralized iot security and standards*, San Diego, CA. Reston, VA, 2018. URL: https://doi.org/10.14722/diss.2018.23007 (date of access: 26.01.2024).

21. Leveraging software-defined networking for security policy enforcement / J. Liu et al. *Information sciences*. 2016. Vol. 327. P. 288–299. URL: https://doi.org/10.1016/j.ins.2015.08.019 (date of access: 26.01.2024).

22. Neisse R., Steri G., Baldini G. Enforcement of security policy rules for the Internet of Things. *2014 IEEE 10th international conference on wireless and mobile computing, networking and communications (wimob)*, Larnaca, Cyprus, 8–10 October 2014. 2014. URL: https://doi.org/10.1109/wimob.2014.6962166 (date of access: 26.01.2024).

23. Hu F., Hao Q., Bao K. A survey on software-defined network and openflow: from concept to implementation. *IEEE communications surveys & tutorials*. 2014. Vol. 16, no. 4. P. 2181–2206. URL: https://doi.org/10.1109/comst.2014.2326417 (date of access: 26.01.2024).

24. Wang B., Lu K., Chang P. Design and implementation of Linux firewall based on the frame of Netfilter/IPtable. *2016 11th international conference on computer science & education (ICCSE)*, Nagoya, Japan, 23–25 August 2016. 2016. URL: https://doi.org/10.1109/iccse.2016.7581711 (date of access: 26.01.2024).

25. Zheng S., Li Z., Li B. Implementation and application of ACL in campus network. *11th asian conference on chemical sensors: (accs2015)*, Penang, Malaysia. 2017. URL: https://doi.org/10.1063/1.4977398 (date of access: 26.01.2024).

26. An enhanced WLAN security system with FPGA implementation for multimedia applications / T. Hayajneh et al. *IEEE systems journal*. 2017. Vol. 11, no. 4. P. 2536–2545. URL: https://doi.org/10.1109/jsyst.2015.2424702 (date of access: 26.01.2024).

27. Ali M., Khan S. U., Vasilakos A. V. Security in cloud computing: opportunities and challenges. *Information sciences*. 2015. Vol. 305. P. 357–383. URL: https://doi.org/10.1016/j.ins.2015.01.025 (date of access: 26.01.2024).

28. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: a survey / P. Sinha et al. *2017 international conference on signal processing and communication (ICSPC)*, Coimbatore, 28–29 July 2017. 2017. URL: https://doi.org/10.1109/cspc.2017.8305855 (date of access: 26.01.2024).

29. Kang M.-J., Kang J.-W. A novel intrusion detection method using deep neural network for in-vehicle network security. *2016 IEEE 83rd vehicular technology conference (VTC spring)*, Nanjing, China, 15–18 May 2016. 2016. URL: https://doi.org/10.1109/vtcspring.2016.7504089 (date of access: 26.01.2024).

30. Dastres R., Soori M. Secure socket layer (SSL) in the network and web security. *ResearchGate*. URL: https://www.researchgate.net/publication/344781801_Secure_Socket_Layer_SSL_in_the_Network_and_Web_Security.

31. Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers / S. Climent et al. *Sensors*. 2014. Vol. 14, no. 1. P. 795–833. URL: https://doi.org/10.3390/s140100795 (date of access: 26.01.2024).

32. Network layers threats & its countermeasures in wsns / V. Pruthi et al. *2019 international conference on computing, communication, and intelligent systems (ICCCIS)*, Greater Noida, India, 18–19 October 2019. 2019. URL: https://doi.org/10.1109/icccis48478.2019.8974523 (date of access: 26.01.2024).

33. Five-Layers sdp-based hierarchical security paradigm for multi-access edge computing / J. Singh et al. *ResearchGate*. URL: https://www.researchgate.net/publication/342655712_Five-Layers_SDP-Based_Hierarchical_Security_Paradigm_for_Multi-access_Edge_Computing.

34. Capturing the security effects of network segmentation via a continuous-time markov chain model / N. Wagner et al. *ANSS '17: proceedings of the 50th annual simulation symposium*. 2017. P. 1–12. URL: https://dl.acm.org/doi/10.5555/3106388.3106405.

35. SegGuard: segmentation-based anonymization of network data in clouds for privacy-preserving security auditing / M. Oqaily et al. *IEEE transactions on dependable and secure computing*. 2021. P. 1. URL: https://doi.org/10.1109/tdsc.2019.2957488 (date of access: 26.01.2024).

36. Efficient weakly secure network coding scheme against node conspiracy attack based on network segmentation / R. Du et al. *EURASIP journal on wireless communications and networking*. 2014. Vol. 2014, no. 1. URL: https://doi.org/10.1186/1687-1499-2014-5 (date of access: 26.01.2024).

37. Bazrafkan S., Thavalengal S., Corcoran P. An end to end Deep Neural Network for iris segmentation in unconstrained scenarios. *Neural networks*. 2018.

Vol. 106. P. 79–95. URL: https://doi.org/10.1016/j.neunet.2018.06.011 (date of access: 26.01.2024).

38. Clincy V., Shahriar H. Web application firewall: network security models and configuration. *2018 IEEE 42nd annual computer software and applications conference (COMPSAC)*, Tokyo, Japan, 23–27 July 2018. 2018. URL: https://doi.org/10.1109/compsac.2018.00144 (date of access: 26.01.2024).

39. Software defined networking reactive stateful firewall / S. Zerkane et al. *ICT systems security and privacy protection*. Cham, 2016. P. 119–132. URL: https://doi.org/10.1007/978-3-319-33630-5_9 (date of access: 26.01.2024).

40. Ben Achballah A., Ben Othman S., Ben Saoud S. FW_IP: A flexible and lightweight hardware firewall for NoC-based systems. *2018 international conference on advanced systems and electric technologies (IC_ASET)*, Hammamet, 22–25 March 2018. 2018. URL: https://doi.org/10.1109/aset.2018.8379868 (date of access: 26.01.2024).

41. Design and implementation of enterprise network security system based on firewall / H. Yuan et al. *Advances in intelligent systems and computing*. Cham, 2019. P. 1070–1078. URL: https://doi.org/10.1007/978-3-030-15235-2_142 (date of access: 26.01.2024).

42. Nasimuzzaman C. M., Ken F., Mike F. Network intrusion detection using machine learning. *Proceedings of the international conference on security and management (SAM)*. 2016. P. 30–35.

43. Cyber attack modeling and simulation for network security analysis / M. E. Kuhl et al. *2007 winter simulation conference*, Washington, DC, USA, 9–12 December 2007. 2007. URL: https://doi.org/10.1109/wsc.2007.4419720 (date of access: 26.01.2024).

44. Tree formation with physical layer security considerations in wireless multi-hop networks / W. Saad et al. *IEEE transactions on wireless communications*. 2012. Vol. 11, no. 11. P. 3980–3991. URL: https://doi.org/10.1109/twc.2012.091812.111923 (date of access: 26.01.2024).

45. Dini G., Tiloca M. Considerations on security in zigbee networks. *2010 IEEE international conference on sensor networks, ubiquitous, and trustworthy computing*, Newport Beach, CA, USA, 7–9 June 2010. 2010. URL: https://doi.org/10.1109/sutc.2010.15 (date of access: 26.01.2024).

46. Network attacks: taxonomy, tools and systems / N. Hoque et al. *Journal of network and computer applications*. 2014. Vol. 40. P. 307–324. URL: https://doi.org/10.1016/j.jnca.2013.08.001 (date of access: 26.01.2024).

47. Gorodetski V., Kotenko I. Attacks against computer network: formal grammar-based framework and simulation tool. *Lecture notes in computer science*. Berlin, Heidelberg, 2002. P. 219–238. URL: https://doi.org/10.1007/3-540-36084-0_12 (date of access: 26.01.2024).

48. Alfaro J. G., Boulahia-Cuppens N., Cuppens F. Complete analysis of configuration rules to guarantee reliable network security policies. *International journal of information security*. 2007. Vol. 7, no. 2. P. 103–122. URL: https://doi.org/10.1007/s10207-007-0045-7 (date of access: 26.01.2024).

49. Sahana A., Misra I. S. Implementation of RSA security protocol for sensor network security: design and network lifetime analysis. *Electronic systems technology (wireless VITAE)*, Chennai, India, 28 February – 3 March 2011. 2011. URL: https://doi.org/10.1109/wirelessvitae.2011.5940853 (date of access: 26.01.2024).

50. A survey on security issues and solutions at different layers of Cloud computing / C. Modi et al. *The journal of supercomputing*. 2012. Vol. 63, no. 2. P. 561–592. URL: https://doi.org/10.1007/s11227-012-0831-5 (date of access: 26.01.2024).

51. Improving cloud network security using the Tree-Rule firewall / X. He et al. *Future generation computer systems*. 2014. Vol. 30. P. 116–126. URL: https://doi.org/10.1016/j.future.2013.06.024 (date of access: 26.01.2024).

52. Hu H., Ahn G.-J., Kulkarni K. Detecting and resolving firewall policy anomalies. *IEEE transactions on dependable and secure computing*. 2012. Vol. 9,

no. 3. P. 318–331. URL: https://doi.org/10.1109/tdsc.2012.20 (date of access: 26.01.2024).

53. Широчин В. П., Мухин В. Е., Кулик А. В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. Киев : ВЕК+, 2000. 111 с.

54. Ганиев С. К., Каримов М. М. Вопросы оптимального сегментирования топологии локальных компьютерных сетей. *Проблемы информатики и энергетики*. 2001. № 2. С. 20–25.

55. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 4-те вид. СПб : П, 2010. 944 с.

56. Платонов В. В. Программно-аппаратные средства защиты информации. М : Академия, 2006. 240 с.

57. Formation of dependability and cyber protection model in information systems of situational center / V. Grechaninov et al. *ResearchGate*. URL: https://www.researchgate.net/publication/361176272_Formation_of_Dependability_and_Cyber_Protection_Model_in_Information_Systems_of_Situational_Center.

58. Decentralized access demarcation system construction in situational center network / V. Grechaninov et al. *Інституційний репозиторій Київського університету імені Бориса Грінченка*. URL: https://elibrary.kubg.edu.ua/id/eprint/41951/.

59. Tajdini M., Sokolov V., Buriachok V. Men-in-the-Middle attack simulation on low energy wireless devices using software define radio. *ResearchGate*. URL: https://www.researchgate.net/publication/334048676_Men-in-the-Middle_Attack_Simulation_on_Low_Energy_Wireless_Devices_using_Software_Define_Radio.

60. Increasing the functional network stability in the depression zone of the hydroelectric power station reservoir / P. Anakhov et al. *ResearchGate*. URL: https://www.researchgate.net/publication/361176379_Increasing_the_Functional_

Network_Stability_in_the_Depression_Zone_of_the_Hydroelectric_Power_Station_Reservoir.

61. Sakrutina E. Some functions of the “Safety management system” in the transportation area safety assurance. *2017 international siberian conference on control and communications (SIBCON)*, Astana, Kazakhstan, 29–30 June 2017. 2017. URL: https://doi.org/10.1109/sibcon.2017.7998576 (date of access: 26.01.2024).

62. I. Zhukov, S. Balakin. Detection of computer attacks using outliner method. *J. Young Sci.* 2016. Vol. 9, no. 36. P. 91–93.

63. Federal ministry of the interior, building and community (BMI). *MyScience*. URL: https://www.myscience.org/directory/administration/germany/bmi-bund.

64. Kritische Infrastrukturen. *BBK*. URL: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html.

65. Bundesamt für Sicherheit in der Informationstechnik. *BSI*. URL: https://www.bsi.bund.de/DE/Home/home_node.html.

66. ENISA threat landscape 2020. *ENISA*. URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020.

67. Education. *ENISA*. URL: https://www.enisa.europa.eu/topics/education (date of access: 26.01.2024).

68. Power Sector Dependency on Time Service: attacks against time sensitive services. *ENISA*. URL: https://www.enisa.europa.eu/publications/power-sector-dependency (date of access: 26.01.2024).

69. Scarfone K., Mell P. Guide to intrusion detection and prevention systems (IDPS). *NIST*. URL: https://doi.org/10.6028/NIST.SP.800-94.

70. Methods of risk assessment for information security management / M. Al Hadidi et al. *International review on computers and software (IRECOS)*.

2016. Vol. 11, no. 2. P. 81. URL: https://doi.org/10.15866/irecos.v11i2.8233 (date of access: 26.01.2024).

71. Zhukov I. Implementation of integral telecommunication environment for harmonised air traffic control with scalable flight display systems. *Aviation*. 2010. Vol. 14, no. 4. P. 117–122. URL: https://doi.org/10.3846/aviation.2010.18 (date of access: 26.01.2024).

72. Zhukov I. Increasing the accuracy of the information load annual growth evaluation on the internet of things. *ceur-ws.org*. URL: https://ceur-ws.org/Vol-2588/paper49.pdf.

73. Gnatiuk S. Y. Study on complex assessment of the information and communication systems efficiency. *ceur-ws.org*. URL: https://ceur-ws.org/Vol-2654/paper53.pdf.

74. Avkurova Z., Gnatyuk S., Abduraimova B. Structural and analytical models for early apt-attacks detection in critical infrastructure. *Communications in computer and information science*. Cham, 2022. P. 455–468. URL: https://doi.org/10.1007/978-3-031-14841-5_30 (date of access: 26.01.2024).

75. Gnatyuk S. Method for calculating the criticality level of sectoral information and telecommunication systems. *ceur-ws.org*. URL: https://ceur-ws.org/Vol-3347/Paper_20.pdf.

76. Gnatyuk S. Critical aviation information systems cybersecurity. *Meeting security challenges through data analytics and decision support. NATO science for peace and security series. D: information and communication security*. 47th ed. 2016. P. 308–316.

77. Gnatyuk S. Studies on cloud-based cyber incidents detection and identification in critical infrastructure. *ceur-ws.org*. URL: https://ceur-ws.org/Vol-2923/paper8.pdf.