DOI 10.31891/2307-5732-2023-321-3-120-127
УДК 632:654.672

ЛЕМЕШКО АНДРІЙ
Державний університет телекомунікацій
ORCID ID: 0000-0001-8003-3168
АНТОНЕНКО АРТЕМ
Державний університет телекомунікацій
ORCID ID: 0000-0001-9397-1209
e-mail: artem.v.antonenko@gmail.com
КУВІК НАЗАР
Державний університет телекомунікацій
ORCID ID: 0009-0008-0983-7110
ГНЯДИЙ ВЛАДИСЛАВ
Державний університет телекомунікацій
ORCID ID: 0009-0001-6866-3922

ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ ЗАГРОЗ ДЛЯ ЗАБЕЗПЕЧЕННЯ МАКСИМАЛЬНОГО ЗАХИСТУ ДАНИХ ТА ІНФРАСТРУКТУРИ

Мережі є системами, вразливими для зловмисників, оскільки їх основною функцією є полегшення віддаленого доступу та передачі даних. У розвитку технологій та збільшенні кількості підключених до мереж пристроїв, зростає кількість потенційних загроз для безпеки мережі. Це ставить перед інформаційними технологіями завдання постійного підвищення рівня безпеки мережі та зменшення вразливості до атак. Інформація в мережах має бути безпечною, щоб забезпечити ефективний зв'язок та обмін даними в мережі. Через проблеми та загрози для даних у мережах безпека мережі є одним із найважливіших аспектів інфраструктури інформаційних технологій. У зв'язку з тим, що безпека є однією з головних потреб в інфраструктурі інформаційних технологій, протягом багатьох років різні вчені проводили дослідження в цій області. У результаті під час побудови мережі розробляються заходи безпеки мережі, щоб зменшити можливість хакерів отримати доступ до захищених даних. Метою безпеки мережі є захист мережі та її компонентів від несанкціонованого доступу та зловживань, щоб надати користувачам безпечний та безпечний зв'язок. У цій статті представлено огляд останніх розробок у сфері мережевих загроз і заходів безпеки, а також перспективні напрямки досліджень. У статті розглядаються різні мережеві атаки та засоби підвищення безпеки мережевих даних. На основі аналізу останніх досліджень у цій статті обговорюються основні типи та категорії мережевих загроз і атак, яким піддається мережа. Наведено їх класифікацію та проведено детальний аналіз ознак. Цілі безпеки мережі можна представити трьома категоріями: підтвердження конфіденційності даних, підтримка повних даних, підтримка доступності даних. Велика увага приділяється методам захисту мереж від несанкціонованого доступу та впливу мережевих загроз. Базуючись на огляді досліджень мережевої безпеки, у статті наводиться перелік ефективних заходів безпеки мережі для запобігання мережевим вторгненням. У статті також наголошується на важливості своєчасного виявлення та реагування на мережеві загрози, щоб забезпечити найвищий рівень безпеки передачі даних в мережі. Розробка та застосування ефективних методів захисту є критичним елементом для забезпечення безпеки мереж та їх користувачів. Таким чином, нові ідеї в системах мережевої безпеки можуть бути представлені через аналіз опублікованих робіт для подальших досліджень.

Ключові слова: мережева безпека, захищені дані, типи і категорії загроз та атаки, заходи безпеки, запобігання вторгненням, апаратні брандмауери, програмні брандмауери, рівні безпеки мережі.

LEMESHKO ANDRIY
State University of Telecommunications
ANTONENKO ARTEM
State University of Telecommunications
KUVIK NAZAR
State University of Telecommunications
HNIADYI VLADYSLAV
State University of Telecommunications

INVESTIGATING NETWORK THREATS TO ENSURE MAXIMUM PROTECTION OF DATA AND INFRASTRUCTURE

Networks are systems vulnerable to attackers because their main function is to facilitate remote access and data transfer. With the development of technology and the increase in the number of devices connected to networks, the number of potential network security threats is growing. This challenges information technology to continuously improve network security and reduce attack vulnerabilities. Information on networks must be safe and secure to enable efficient communication and data exchange on the network. Due to the challenges and threats to data in networks, network security is one of the most important aspects of an information technology infrastructure. Due to the fact that security is one of the main needs in information technology infrastructure, scientists have been conducting research in this area for many years. As a result, when building a network, network security measures are designed to reduce the ability of hackers to gain access to protected data. The goal of network security is to protect the network and its components from unauthorized access and abuse in order to provide users with safe and secure communications. This article provides an overview of recent developments in the field of network threats and security measures, as well as promising areas of research. The article discusses various network attacks and ways to improve the security of network data. Based on the analysis of recent research, this article discusses the main types and categories of network threats and attacks to which the network is exposed. Their classification is given and a detailed analysis of the features is carried out. Network security objectives can be provided in three categories: data confidentiality assurance, complete data

maintenance, data availability maintenance. Much attention is paid to methods of protecting networks from unauthorized access and the impact of network threats. Based on a review of network security research, the article provides a list of effective network security measures to prevent network intrusions. The article also notes the importance of timely detection and response to network threats in order to ensure a high level of data transmission security on the network. The development and application of effective protection methods is a critical element in ensuring the security of networks and their users. Thus, new ideas in network security systems can be presented through the analysis of published works for further research.

Keywords: network security, protected data, types and categories of threats and attacks, security measures, intrusion prevention, hardware firewalls, software firewalls, network security levels.

Постановка проблеми

З розширенням залежності бізнес-систем від інфраструктури IT-систем мережева безпека на сьогоднішній день є однією з найважливіших вимог в галузі інформаційної безпеки. Відсутність заходів безпеки в IT-інфраструктурі може завдати непоправної шкоди організаціям та компаніям, що є небажаним для бізнесу та маркетингового процесу. Метою мережевої безпеки є насамперед запобігання шкоді від неправильного використання даних. Існує низка потенційних проблем, які можуть виникнути, якщо мережева безпека не реалізована належним чином. Кожній комерційній установі необхідно приховувати певну важливу та таємну інформацію від доступу своїх конкурентів. Втрата даних може знизити додану вартість у процесі виробництва та продажу товарів. Більш того, справжній шлях руху в комерційній діяльності та маркетингу продуктів може бути втрачений через маніпулювання даними внаслідок відсутності заходів безпеки у фінансовій інформації. В результаті відсутність заходів безпеки в мережі даних може дуже важливо використовувати суворі принципи для запобігання можливим втратам, незалежно від розміру та типу мережі [1]. Це набір принципів, правил і заходів, розроблених мережним адміністратором або адміністраторами для запобігання та моніторингу несанкціонованого доступу, неправильного використання, виправлення, запобігання змінам або обмеження доступу до комп'ютерних мереж та доступних мережевих ресурсів [2].

Аналіз останніх джерел

У цій роботі розглянуто та класифіковано питання дослідження мережевих загроз і заходів безпеки з метою захисту мереж від несанкціонованого доступу. Проведення аналітичного огляду останніх досліджень стосовно мережевих загроз та вироблення заходів безпеки від них є актуальним завданням, розв’язання якого дозволить зменшити доступ зловмисників до захищених даних та отримати надійну систему мережевої безпеки [3–7].

Значний внесок у вирішення фундаментальних питань у сфері мережевих загроз і заходів мережевої безпеки є дослідження таких вітчизняних та зарубіжних вчених: В.Б. Толубка, В.Л. Бурячка, С. В. Толюпи, В.А. Козачка, Г.І. Гайдур, М.В. Грайворонського, B. Gupta, M. Wazid, H. I. Kobo, M. Stawowski, D. Barrera, R. Neisse, B. Wang та ін. [1–24].

Метою роботи є аналітичний огляд та систематизація мережевих загроз і визначення стратегії ефективних засобів для забезпечення мережевої безпеки.

Об’єкт дослідження – методи та засоби забезпечення мережевої безпеки.

Предмет дослідження – типи та категорії загроз для мережевої безпеки, класифікація різних атак на захищені мережі.

Виклад основного матеріалу

У зв'язку з тим, що безпека є однією з основних потреб в інфраструктурі інформаційних технологій, у різних науково-дослідних роботах було проведено велике дослідження в цьому напрямку. Щоб забезпечити заходи безпеки в мережі даних, атаки мають бути чітко визначені. Атака – це небезпечна чи безпечна спроба змінити або використовувати ресурс, доступний через мережу, не за призначенням. Мережеві атаки можна розділити на три основні категорії:

1) Несанкціонований доступ до ресурсів та інформації через мережу.

2) Несанкціоноване маніпулювання інформацією мережі.

3) Атаки, які призводять до порушення надання послуг та називається відмовою в обслуговуванні.

Визначення санкціонованої чи несанкціонованої дії є обов'язком політики мережної безпеки, яка може бути визначена як спроба користувача переглянути чи змінити заборонену інформацію. Несанкціонований доступ може бути однією з найпоширеніших атак у будь-якій мережі. Таким чином зловмисник намагається отримати доступ до зони обмеженого доступу до інформації та мережі. Злом паролів, створення фальшивих ідентифікаторів або використання зловмисного програмного забезпечення є основними способами здійснення цих атак [4, 5].

Знищення інформації є однією з найбільш руйнівних атак мережі. Таким чином зловмисник намагається знищити певну інформацію, виконуючи команди в базі даних. Це може бути обмеженим або дуже великим. Залежно від типу зловмисника, мережа може втратити всю інформацію за лічені секунди. Атаки, які призводять до порушення надання послуг, є ще однією формою несанкціонованого доступу. У цьому випадку особа входить в область користувача або керування для виконання команди або набору команд, які зазвичай є забороненими. Таким чином зловмисник може вводити, змінювати, надсилати електронною поштою, копіювати інформацію або видаляти певну інформацію, щоб знайти спосіб доступу до даних з обмеженим доступом. Ступінь атаки залежить від можливостей зловмисника [6, 7].

Загрози мережевої безпеки потрапляють до однієї чи двох загальних категорій, таких як логічні

атаки або атаки з регресом. Раціональні атаки, як випливає з назви, є комерційною стратегією, яка використовується для усунення будь-яких недоліків у системі. До недоліків можна віднести вразливість програмного забезпечення, таку як комп'ютерний дефект, який дозволяє обійти систему захисту, та помилки безпеки в коді. Метою атаки є проникнення в систему з метою пошкодження чи отримання несанкціонованого доступу до системи [8, 9].

Ресурсні атаки спрямовано на знищення ресурсів мереж. Цей прийом став популярним у 1990-х роках, але поступово його популярність знизилася. При цьому методі мережева система примусово руйнується, що робить її вразливою. Ці атаки здійснюються по-різному, щоб застосувати зусилля для доступу до інтернет даних. Найшвидший спосіб для сервера – зіткнутися з величезним потоком запитів на обслуговування, що знаходяться поза його контролем. Також деякі ресурсні атаки 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. Щоб ідентифікувати мережу, зловмисник контролює мережу організації. Оскільки в цій атаці зловмисник не робить ніяких зловмисних дій, виявити цей тип атаки дуже складно, наприклад, один тип пасивної атаки полягає в тому, що зловмисник захоплює внутрішні мережеві пакети організації. Протидія цій атаці полягає в тому, що цей тип атаки легко запобігти за допомогою належного шифрування в інфраструктурі мережі [11].

- *Активні атаки*: при цьому типі атак зловмисник безпосередньо атакує сервери організації. Атаки відстежуються системою безпеки мережі. Стратегії боротьби з цими атаками включають встановлення брандмауерів (програмних та апаратних), а також систем IPS [11, 12].

- *Внутрішні атаки*: при цьому типі атак зловмисники отримують фізичний доступ до систем. На жаль, при фізичному доступі до систем практично будь-який зловмисник може зробити велику роботу і завдати непоправної шкоди організації. Відповідним та логічним способом боротьби з цим типом атак є забезпечення фізичної безпеки систем та серверів [12].

- *Внутрішні атаки користувачів організацій*: Ці типи мережевих атак зазвичай здійснюються внутрішніми користувачами організацій, які мають доступ до систем та інформації. Залежно від рівня знань та обізнаності зловмисників про комп'ютерні мережі, вони можуть проникнути до мережних систем. Боротьба з атаками полягає у запобіганні цьому типу атак безпеки на рівні 2 і зосередитися на автентифікації, у той час як фізична безпека має бути повністю забезпечена [12, 13].

У сучасній мережі є багато ресурсів для захисту мережі. Нижче наведено список мережевих ресурсів, які мають бути захищені від усіх типів атак:

- міжмережеві екрани, маршрутизатори та комутатори в якості мережевого обладнання;

- інформація про роботу мережі, така як таблиці маршрутизації та конфігурації списків доступу, що зберігаються на маршрутизаторі;

- нематеріальні мережеві ресурси, такі як пропускна здатність та швидкість;

- інформація та інформаційні ресурси, підключені до мережі, такі як бази даних та інформаційні сервери;

- термінали, які підключені до мережі для використання різних джерел;

- інформація, якою обмінюються в мережі у будь-який момент часу;

- конфіденційність операцій користувачів та використання їх мережевих ресурсів для запобігання ідентифікації користувача [14, 15].

На мережевих комп'ютерах, таких як бази даних та веб-сервери, в мережі відбувається обмін інформацією та інформацією про мережеві компоненти для виконання таких завдань, як таблиці маршрутизації маршрутизатора. Мережеві ресурси також можуть бути термінальним обладнанням, таким як маршрутизатори та брандмауери, або механізмами підключення для запобігання доступу хакерів до захищених даних [16].

Для реалізації передових систем безпеки в мережі даних до заходів безпеки мереж слід застосовувати належні методи і принципи проектування. Ключові заходи захисту для мережної безпеки включають брандмауери, виявлення вторгнень та брандмауер веб-додатків, систему виявлення вторгнень (IDS) та систему запобігання вторгнень (IPS), захист віртуальної приватної мережі (VPN) та перегляд контенту – фільтрацію спаму та унікальний механізм вказівки місцезнаходження ресурсів. [17]. Ці апаратні та програмні рішення, що підтримують та доповнюють механізми безпеки для операційних систем, баз даних та додатків. Для забезпечення ефективної системи захисту даних у надійній мережі застосовуються методи проектування за рівнями загроз [18].

Основні принципи безпеки IT-систем, які повинні розглядатись при проектуванні системи мережевої безпеки, показано на рисунку 1 [19].

Політика безпеки мережі має бути визначена таким чином, щоб мінімізувати ризик і суму збитку після аналізу ризику в мережі даних. Політика безпеки має бути загальною і в полі загального бачення і не вдаватися в деталі. Деталі можуть змінитися за короткий час, а її політика залишається незмінною.

Елементами політики безпеки є такі питання: що і чому дані повинні бути захищені, хто відповідає за захист даних, створення контексту, який вирішує будь-які можливі конфлікти.

Політики безпеки можна умовно розділити на дві категорії: дозвільна (все, що явно не заборонено, дозволено) та обмежена (все, що явно не дозволено, заборонено). Зазвичай ідея використання

обмежувальної політика безпеки є кращою та доцільнішою з точки зору підвищення безпеки мережевих систем. Цей вибір викликаний проблемами безпеки авторизованих політик для забезпечення обмеження доступу до захищених даних [20].

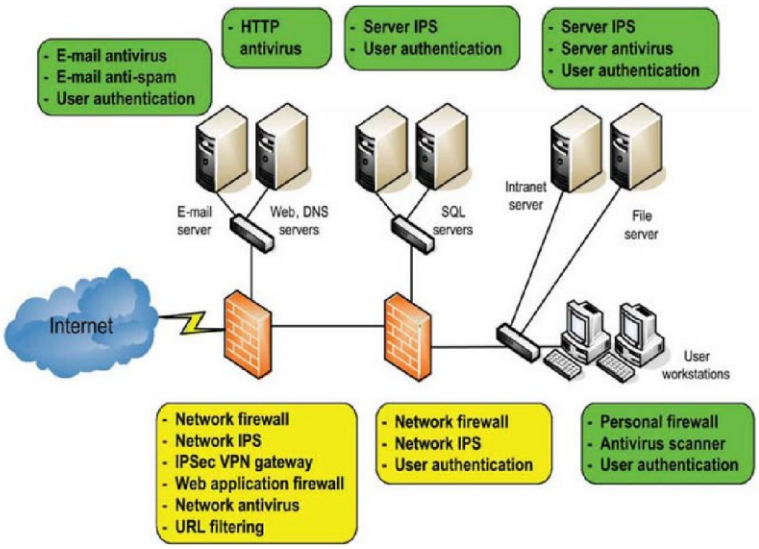

Рис. 1. Принцип комплексного захисту різних ресурсів IT-системи на основі кількох взаємодоповнюючих рівнів безпеки

Найкращий підхід до забезпечення надійної мережевої безпеки – повна підготовка мережі до загроз. Існують 4 типи процесів реалізації безпеки мережі:

- безпека: відомості про те, що всі компоненти є надійним чином ліцензовані та мають політики автентифікації та захисту;

- огляд: відстеження мережевих дій та безперервність дій із захисту;

- тестування: оцінка вразливостей політик безпеки, призначених для мережі, шляхом імітації атаки довіреною особою;

- покращання ситуації: на основі всіх попередніх кроків необхідно зібрати дані та використовувати їх для створення якісніших заходів [21].

Усі мережеві адміністратори повинні мати на увазі, що добра стратегія безпеки мережі передбачає постійний моніторинг і обслуговування. Звичайно, недостатньо лише розроблення політики безпеки, Нападники постійно вдосконалюються, щоб знайти шлях до захищених даних. Отже, мережеві адміністратори повинні бути в курсі цих вдосконалень [22].

Усунення небезпеки : після визначення мережевих активів та їхніх загрозливих факторів слід оцінити різні ризики. У кращому випадку мережа повинна мати можливість захистити від усіх видів помилок, але дешевої безпеки не досягти. Тому необхідно правильно оцінити типи ризиків, щоб визначити найважливіші з них, а з іншого боку, щоб визначити джерела, від яких слід захистити ці ризики. Існують два основні фактори в аналізі ризику: можливість здійснення нападу та пошкодження мережі у разі успішної атаки.

Рівні мережі: рівні безпеки є класифікацією мережевих дій, щоб кожна мережева діяльність могла бути захищена окремо та політики безпеки одного рівня не впливали на параметри безпеки іншого рівня.

Рівні безпеки мережі дозволяють перевірити безпеку кожної діяльності окремо шляхом класифікації мережевої діяльності та розміщення їх на різних рівнях. Оскільки кожна діяльність розглядається окремо, можна точно керувати заходами безпеки на кожному рівні.

Щоб збільшити рівень безпеки комплексної IT-інфраструктури, рішення безпеки мають використовуватися на всіх рівнях IT-архітектури підприємства. Щоб встановити наскрізну безпеку, необхідно застосовувати компоненти безпеки, що стосуються різного обладнання та груп. Завдання рівнів безпеки, як мережевих рівнів, полягає в наданні послуг і активації вищого рівня. Таким чином, потреба в багаторівневій мережі відчувається в веб-даних.

Рівень безпеки інфраструктури: рівень інфраструктури охоплює безпеку об'єктів передавальної мережі та окремих мережевих інструментів. Цей рівень дає змогу ознайомитись з основною реалізацією мережі, служб та додатків.

Рівень безпеки програмних додатків: цей режим фокусується на програмах, доступних для користувачів в Інтернеті. Мережні програми можуть бути перевірені в постачальниках послуг додатків (ASP), таких як третій серверний центр обслуговування, серверний сервер, який сам вибирає ASP, або в хост-компаніях, які можуть бути незалежними в цьому центрі. Згідно з цим рівнем, можуть бути сприйняті як загроза чотири цілі: користувачі додатків, постачальник програм, суб-провайдер, постачальник послуг. Структура рівня безпеки програмних додатків в рамках безпеки мережі представлена на рисунку 2.

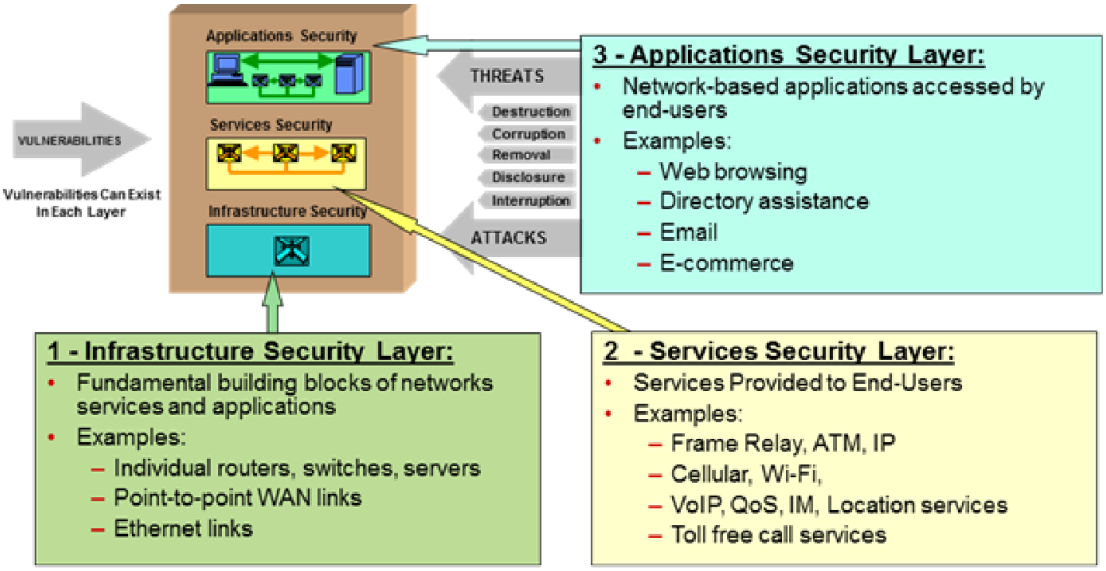

Рис. 2. Структура рівня безпеки програмних додатків в рамках безпеки мереж

Контрольний рівень безпеки: функція цього рівня полягає в тому, щоб виконувати допоміжні дії, що відповідають за передачу інформацію про послуги або мережеві програми. Цей рівень зазвичай включає зв'язок між машинами у мережі, яка зазвичай включає управляюче повідомлення.

Рівень безпеки на стороні користувача: цей рівень безпеки включає власну функцію захисту та перевірки послуг, що надаються провайдером на стороні користувача. Кінцеві користувачі можуть використовувати постачальника послуг самої мережі або послуг розширення, таких як VPN.

Сегментація інформації: ресурси IT-системи з різним рівнем і чутливістю, включаючи толерантність до ризику та вразливість до різних ступенів загрози повинна бути включена до різних зон безпеки. Принцип «приховування інформації» розглядається як один з розширених випадків цього правила, так що IT-системи лише надають дані, необхідні для виконання завдань IT-системи.. Система може бути заблокована як сервер для обслуговування інтернет-провайдерів, які зареєстровані лише у загальнодоступних DNS. Принцип мінімальної кількості балів для людей, підключених до IT-системи (таких як користувачі та системні адміністратори) повинен надавати мінімальні привілеї, необхідні для оптимальної продуктивності в організації. Це також стосується і даних та послуг, які є доступними для зовнішніх користувачів. Одним із розширень цього правила є принцип «необхідності знати», згідно з яким користувачі та керівники IT системи мають доступ лише до інформації, що стосується їх ролей та завдань [23].

Рівень безпеки IT-системи залежить від фактору, який має найменшу безпеку. Одним із розширень цього правила є принцип єдиної точки відмови (SPOF), який пов'язаний з доступністю мережевих послуг, згідно з яким всі сполучні ланки, обладнання (мережі та безпеки), а також сервери на мережевих маршрутах між користувачами та в функціональні характеристики важливих ресурсів IT-системи повинні бути реалізовані в надлишкові конфігурації. При проектуванні системи захисту мережі повинні бути розглянуті принципи організаційної безпеки, в тому числі правила «розподілу обов'язків» і "робочий процес". Метою цих принципів є обмеження здатності співробітників ігнорувати та порушувати політику безпеки IT-системи. Розподіл обов'язків означає, що важливі завдання і функції повинні виконуватися двома або більшою кількістю працівників. Також плинність робочих кадрів слід враховувати для важливих робочих посад з точки зору заходів безпеки мережі.

Ресурси IT-систем різного рівня чутливості повинні бути розташовані в різних зонах безпеки. Комп'ютерне обладнання та постачальники послуг для зовнішніх мереж (такі як інтернет-провайдери) повинні бути розташовані в різних зонах (таких як демілітаризована зона), на відміну від комп'ютерних систем і внутрішнього мережевого обладнання. Стратегічні ресурси IT-системи повинні бути розташовані в певному конкретному місці зони безпеки, яким необхідно забезпечити захист [21]. Комп'ютерне обладнання з низькою надійністю та системи, такі як сервери віддаленого доступу та в точки доступу до бездротової мережі слід також слід включати в певні конкретні зони безпеки. Різні типи ресурсів IT-системи повинні бути розміщені в окремих зонах безпеки. Робочі станції для користувачів повинні знаходитися в різних зонах безпеки, на відміну від серверів. Системи безпеки та управління мережею повинні бути розташовані в певних конкретних зонах безпеки. Системи на етапі розробки повинні бути розміщені в іншому секторі, на відміну від систем пов'язаних з виробничою фазою [22].

Міжмережеві екрани в програмних та апаратних системах діють як стіни безпеки між користувачами мереж та зовнішнім світом. Брандмауери зазвичай розташовані на межі між мережею та Інтернетом. Апаратні брандмауери можуть контролювати контент і комунікаційні шляхи мережі. Брандмауери визначають правила надходження інформації та визначення того, які дані мають право на вхід і вихід а які не мають право. Програмні брандмауери економічно вигідні інструменти в системах

брандмауерів, які дозволяють досліджувати шаблони і водночас можуть забезпечувати контроль за загрозами. Апаратні брандмауери є більш надійними і можуть бути ефективнішими, але менш функціональними ніж їх програмні брандмауери. На розсуд користувача брандмауер є основним інструментом для підтримання або обмеження потоку мережевого трафіку в різних ситуаціях, такі як спеціальне обладнання брандмауера, функція брандмауера в обладнанні IPS і список контролю доступу в мережеві комутатори та маршрутизатори. При правильному розгортанні і конфігурації брандмауери можуть допомогти створити безпечні архітектури, розділити інфраструктуру IT-мережі на домени безпеки та контролювати комунікацію між ними [24].

Для посилення кібератаки на захищені дані було розроблено вдосконалену систему виявлення вторгнень IDS. В цій роботі представлено моделювання вдосконаленої кібератаки для запобігання доступу хакерів до захищені дані в мережах. Віруси, хробаки та трояни намагаються поширюватися по мережі та можуть залишатись на інфікованих пристроях протягом днів або тижнів. Робота системи безпеки полягає в тому, щоб вжити заходів безпеки, для запобігання проникненню такого типу шкідливого програмного забезпечення, а також шкідливого програмного забезпечення, яке відкриває їм шлях. На рисунку 3 показано виконання мережевих процесів безпеки для того, щоб запобігти вторгненню, що контролює взаємодію користувачів з доступом до внутрішньої мережі. У цьому випадку Інтернет-послуги для внутрішніх користувачів доступні через корпоративну електронну пошту та проксі-сервери Hyper Text Transfer Protocol (HTTP).

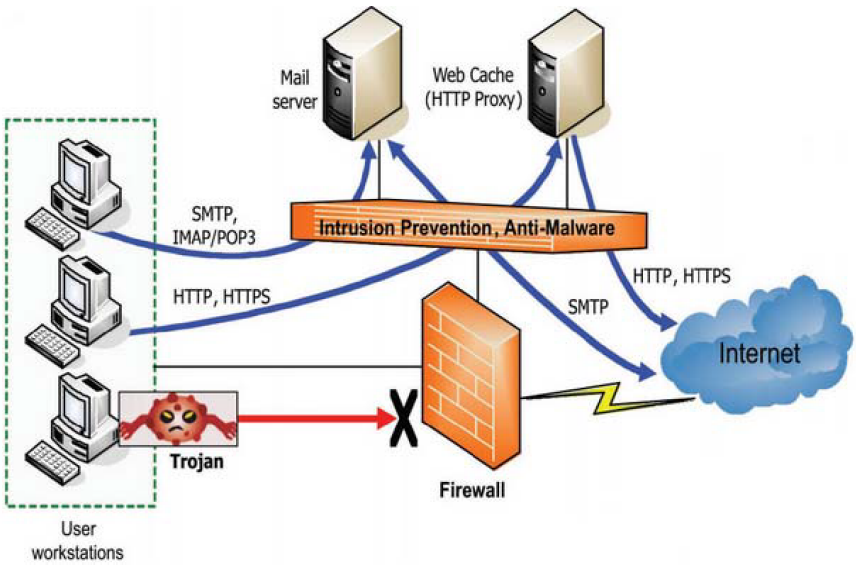

Рис. 3. Приклад схеми для запобігання вторгненням шляхом контролю взаємодії користувачів з доступом до внутрішньої мережі [19]

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

1) захист: потрібно налаштувати системи та мережі належним чином;

2) виявлення: необхідно повністю контролювати мережу та виявляти зміни та використання мережевих ресурсів, які є ознаками вторгнення;

3) реакція: після виявлення проблем необхідно швидко реагувати та швидко та швидко забезпечити безпечне середовище в мережі.

Це є стратегія захисту від зловмисників. Якщо є один спільний знаменник серед експертів з безпеки, небезпечно покладатися на єдину лінію захисту, оскільки будь-який засіб захисту може бути знищений зловмисником. Мережа є не лінія чи точка, а насправді є територією. В результаті, якщо зловмисник атакував частину захищених даних, можливо зберегти ресурси даних і врятувати їх, якщо система безпеки правильно організована. Рішення мережевої безпеки можна доповнити такими заходами:

1) Оцінка ризиків і вразливостей, аналіз і підбір відповідних контролерів.

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

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

4) Консультації щодо вибору правильних стандартів безпеки.

5) Консультації щодо визначення та застосування керівних принципів та виконання інструкції з захисту інформації.

6) Практичне навчання на місці або періодично на різних рівнях.

7) Перевірка міцності систем безпеки шляхом спроб їх зламу.

Висновки

Безпека мережі процес, який певною мірою захищає мережу від різних типів внутрішніх і зовнішніх загроз. Метою безпеки мережі є захист її від зазначених вище атак, тому цілі безпеки мережі можуть бути представлені трьома категоріями: доказ конфіденційності даних, підтримка вичерпних даних, підтримка доступності даних. Для безпеки мережі здійснені наступні кроки: визначено частину, яка має бути захищена; визначено випадки, від яких дана частина має бути захищена; визначено можливі загрози; впроваджено засоби, які можуть захистити активи економічно ефективним способом; постійний контроль процесу і покращання його у разі вразливості. Реалізація політики безпеки досягається у формі плану безпеки мережі. Елементи, з яких складається план безпеки мережі, наступні: функції безпеки кожного пристрою, такі як керуючий пароль або за допомогою Secure Shell (SSH); брандмауери, інтегратори VPN для віддаленого доступу: виявлення вторгнення, сервери безпеки, служби AAA для мережі, механізми контролю та обмеження доступу для різних мережевих пристроїв. Для зниження швидкості вторгнення у захищені дані може бути реалізована удосконалена система моніторингу засобів безпеки. Для захисту даних мають бути передбачені нові протоколи та правила для заходів безпеки різної організації щодо нових рівнів атак на мережі. Для забезпечення розширених заходів безпеки даних мережі можуть бути модифіковані апаратні засоби систем мережевої безпеки. Удосконалення моделей апаратного процесора та програмного забезпечення системи зв'язку для виявлення та запобігання мережевим атакам можна реалізувати в рамках процесу підвищення безпеки мережі.

Література

1. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник ; за заг. ред. В. Б. Толубка. К. : ДУТ, 2015. 288 с.

2. Бурячок В. Л., Толюпа С.В., Семко В.В., Бурячок Л.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник. К. : ДУТ - КНУ, 2016. 178 с.

3. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки : навчальний посібник для студентів вищих навчальних закладів**.** Київ : ДУТ НІІЗІ, 2020. 167 с.

4. Tayal S., Gupta N., Gupta P., Goyal D. and Goyal M. A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, vol. 10 (5), pp. 763-770, 2017.

5. Khan R. and Hasan M. Network threats, attacks and security measures: A review. International Journal of Advanced Research in Computer Science, vol. 8 (8), pp. 116-120, 2017.

6. Rathore S., Sharma P. K., Loia V., Jeong Y.S., Park, J. H. Social network security: Issues, challenges, threats, and solutions. Information sciences, vol. 421. pp. 43-69, 2017.

7. Твердохліб А.О., Коротін Д.С. Ефективність функціонування комп'ютерних систем при використанні технології блокчейн і баз даних. Таврійський науковий вісник. Серія: Технічні науки, 2022, (6).

8. Цвик О.С. Аналіз і особливості програмного забезпечення для контролю трафіку. Вісник Хмельницького національного університету. Серія: Технічні науки, 2023, (1).

9. Новіченко Є.О. Актуальні засади створення алгоритмів обробки інформації для логістичних центрів. Таврійський науковий вісник. Серія: Технічні науки, 2023 (1).

10. Зайцев Є.О. Smart засоби визначення аварійних станів у розподільних електричних мережах міст. Таврійський науковий вісник. Серія: Технічні науки, 2022, (5).

11. Gao S., Li Z., Xiao B. and Wei G. Security threats in the data plane of software-defined networks. IEEE network, vol. 32 (4), pp. 108-113.

12. Islam T., Manivannan D., Zeadally S. A classification and characterization of security threats in cloud computing. Int J Next-Gener Comput, vol. 7 (1), pp. 268-285, 2016.

13. Bays L. R., Oliveira R. R., Barcellos M. P., Gaspary L. P. and Madeira R. M. Virtual network security: threats, countermeasures, and challenges. Journal of Internet Services and Applications, vol. 6 (1), pp. 1, 2015.

14. 14 Sinha P., Kumar Rai A., Bhushan B. Information Security threats and attacks with conceivable counteraction. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). IEEE, pp. 1208-1213, 2019.

15. Dastres R., Soori M. Impact of Meltdown and Spectre on CPU Manufacture Security Issues. vol. 18(2) pp. 62-69, 2021.

16. Tayal A., Mishra N., Sharma S. Active monitoring & postmortem forensic analysis of network threats: A survey. International Journal of Electronics and Information Engineering, vol. 6 (1), pp. 49-59, 2017.

17. Lu Z., Lu X., Wang W. and Wang C. Review and evaluation of security threats on the communication networks in the smart grid. In:2010-Milcom 2010 Military Communications Conference. IEEE, pp. 1830-1835, 2010.

18. Kaynar K. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, vol. 29, pp. 27-56, 2016.

19. Khondoker R., Larbig P., Senf D., Bayarou K, and Gruschka N. AutoSecSDNDemo: Demonstration of automated end-to-end security in software-defined networks. In: 2016 IEEE NetSoft Conference and Workshops

(NetSoft). IEEE, pp. 347-348, 2016.

20. Mahmoud R., Yousuf T., Aloul F. and Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 336-341, 2015.

21. Kobo H. I., Abu-Mahfouz A. M., and Hancke G. P. A survey on software-defined wireless sensor networks: Challenges and design requirements. IEEE access, vol. 5pp. 1872-1899, 2017.

22. Barrera D., Molloy I., and H. Huang H. Standardizing IoT network security policy enforcement. In: Workshop on Decentralized IoT Security and Standards (DISS). p 6, 2018.

23. Wang B., Lu, K. and Chang P. "Design and implementation of Linux firewall based on the frame of Netfilter/IPtable. In: 2016 11th International Conference on Computer Science & Education (ICCSE). IEEE, pp. 949-953, 2016.

24. Zheng S., Li Z. and Li B. Implementation and application of ACL in campus network. In: AIP Conference Proceedings. vol 1. AIP Publishing LLC, p. 090014, 2017.

References

1. Buryachok V. L., Tolubko V. B., Khoroshko V. O., Tolyupa S. V. Information and cyber security: socio-technical aspect; in general ed. V. B. Tolubka. K.: DUT, 2015. 288 p.

2. Buryachok V. L., Tolyupa S. V., Semko V. V., Buryachok L. V., Skladannyi P. M., Lukova-Chuiko N. V. Information and cyberspace: security problems, methods and means of combat. K.: DUT - KNU, 2016. 178 p.

3. Kozachok V.A., Haydur G.I., Gakhov S.O., Khmelevskyi R.M., Chumak N.S. Security policies. Study guide for students of higher educational institutions. Kyiv: DUT NNZI, 2020. 167 p.

4. Tayal S., Gupta N., Gupta P., Goyal D. and Goyal M. A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, vol. 10 (5), pp. 763-770, 2017.

5. Khan R. and Hasan M. Network threats, attacks and security measures: A review. International Journal of Advanced Research in Computer Science, vol. 8 (8), pp. 116-120, 2017.

6. Rathore S., Sharma P. K., Loia V., Jeong Y.S., Park, J. H. Social network security: Issues, challenges, threats, and solutions. Information sciences, vol. 421. pp. 43-69, 2017.

7. Tverdokhlib A.O., Korotin D.S. Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz dannykh. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2022, (6).

8. Tsvyk O.S. Analiz i osoblyvosti prohramnoho zabezpechennia dlia kontroliu trafiku. Herald of Khmelnytskyi National University, 2023, (1).

9. Novichenko Ye.O. Aktualni zasady stvorennia alhorytmiv obrobky informatsii dlia lohistychnykh tsentriv. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2023 (1).

10. Zaitsev Ye.O. Smart zasoby vyznachennia avariinykh staniv u rozpodilnykh elektrychnykh merezhakh mist. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2022, (5).

11. Gao S., Li Z., Xiao B. and Wei G. Security threats in the data plane of software-defined networks. IEEE network, vol. 32 (4), pp. 108-113.

12. Islam T., Manivannan D., Zeadally S. A classification and characterization of security threats in cloud computing. Int J Next-Gener Comput, vol. 7 (1), pp. 268-285, 2016.

13. Bays L. R., Oliveira R. R., Barcellos M. P., Gaspary L. P. and Madeira R. M. Virtual network security: threats, countermeasures, and challenges. Journal of Internet Services and Applications, vol. 6 (1), pp. 1, 2015.

14. 14 Sinha P., Kumar Rai A., Bhushan B. Information Security threats and attacks with conceivable counteraction. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). IEEE, pp. 1208-1213, 2019.

15. Dastres R., Soori M. Impact of Meltdown and Spectre on CPU Manufacture Security Issues. vol. 18(2) pp. 62-69, 2021.

16. Tayal A., Mishra N., Sharma S. Active monitoring & postmortem forensic analysis of network threats: A survey. International Journal of Electronics and Information Engineering, vol. 6 (1), pp. 49-59, 2017.

17. Lu Z., Lu X., Wang W. and Wang C. Review and evaluation of security threats on the communication networks in the smart grid. In:2010-Milcom 2010 Military Communications Conference. IEEE, pp. 1830-1835, 2010.

18. Kaynar K. A taxonomy for attack graph generation and usage in network security. Journal of Information Security and Applications, vol. 29, pp. 27-56, 2016.

19. Khondoker R., Larbig P., Senf D., Bayarou K, and Gruschka N. AutoSecSDNDemo: Demonstration of automated end-to-end security in software-defined networks. In: 2016 IEEE NetSoft Conference and Workshops (NetSoft). IEEE, pp. 347-348, 2016.

20. Mahmoud R., Yousuf T., Aloul F. and Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, pp. 336-341, 2015.

21. Kobo H. I., Abu-Mahfouz A. M., and Hancke G. P. A survey on software-defined wireless sensor networks: Challenges and design requirements. IEEE access, vol. 5pp. 1872-1899, 2017.

22. Barrera D., Molloy I., and H. Huang H. Standardizing IoT network security policy enforcement. In: Workshop on Decentralized IoT Security and Standards (DISS). p 6, 2018.

23. Wang B., Lu, K. and Chang P. "Design and implementation of Linux firewall based on the frame of Netfilter/IPtable. In: 2016 11th International Conference on Computer Science & Education (ICCSE). IEEE, pp. 949-953, 2016.

24. Zheng S., Li Z. and Li B. Implementation and application of ACL in campus network. In: AIP Conference Proceedings. vol 1. AIP Publishing LLC, p. 090014, 2017.