https://doi.org/10.31891/2219-9365-2024-79-26
УДК 004

ЗАГОРУЛЬКО Олександр
Приватний вищий навчальний заклад «Європейський університет»
https://orcid.org/0009-0008-7626-3874

ТЕХНОЛОГІЇ ПОКРАЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ КОМП'ЮТЕРНИХ МЕРЕЖ

Стаття розглядає сучасні технології забезпечення безпеки інформації у комп'ютерних мережах, аналізує методи підвищення захищеності даних від кіберзагроз та оцінює ефективність різних систем захисту. Запропоновано підхід до розробки інтегрованої системи захисту, що включає засоби криптографії, аутентифікації, контролю доступу, а також методи виявлення та запобігання загрозам на основі штучного інтелекту (ШІ). Окремо розглянуто важливість апаратного та програмного захисту, а також питання безпеки в хмарних середовищах.

Ключові слова: захист інформації, комп'ютерні мережі, кібербезпека, криптографія, контроль доступу, штучний інтелект.

ZAHORULKO Oleksandr
Private Higher Educational Institution «European University»

TECHNOLOGIES FOR ENHANCING INFORMATION SECURITY IN COMPUTER NETWORKS

This article examines modern technologies for ensuring information security in computer networks, analyzing methods to strengthen data protection against cyber threats and assessing the effectiveness of various security systems. It proposes an integrated approach to developing a comprehensive protection system that includes cryptography, authentication, and access control, along with threat detection and prevention techniques powered by artificial intelligence (AI). Special attention is given to both hardware and software security solutions, as well as the unique challenges and strategies for maintaining security in cloud environments.

The study begins by exploring foundational concepts in network security, such as the importance of cryptographic methods for safeguarding sensitive data, including encryption and hashing techniques. By encoding information, cryptographic systems make data accessible only to authorized users with the correct decryption keys, offering a robust initial layer of defense. Authentication methods, such as multi-factor authentication (MFA) and biometrics, are also examined as essential measures for verifying user identity, thereby preventing unauthorized access.

The article highlights the role of access control systems, which enforce policies determining user permissions within a network. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are discussed in detail, showcasing how these approaches minimize the risk of unauthorized data access by aligning permissions with organizational roles or specific attributes.

A significant focus is placed on AI-driven threat detection and prevention systems. Machine learning algorithms can analyze network traffic patterns to detect anomalies, which may indicate potential security breaches. This proactive method of identifying suspicious behavior allows systems to react to threats in real time, often mitigating risks before they cause harm.

Finally, the article addresses the growing importance of cloud security. As organizations increasingly rely on cloud services, they must contend with new security considerations, such as shared responsibility between cloud providers and clients. Effective cloud security involves robust encryption, stringent access management, and continuous monitoring to ensure that sensitive data remains protected in a virtualized, highly accessible environment.

Keywords: information security, computer networks, cybersecurity, cryptography, access control, artificial intelligence, cloud security

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Безпека інформації стала одним із ключових викликів сучасного інформаційного суспільства. З кожним роком кількість кіберзлочинів неухильно зростає, а методи й технології атак стають дедалі складнішими й витонченішими. Це створює нагальну потребу в розробці комплексних і адаптивних підходів до захисту даних, що циркулюють у комп'ютерних мережах та використовуються як в особистих, так і в корпоративних цілях.

Надійний захист інформації включає не лише забезпечення захисту від зовнішніх атак, а й створення умов для безпечного зберігання, обробки та передачі даних в межах мережі, незалежно від її масштабу. Особливо важливим є контроль за привілеями доступу користувачів, регулярне оновлення програмного забезпечення, яке мінімізує можливості атак, та впровадження системи моніторингу, що виявляє підозрілу активність у режимі реального часу.

Питання кібербезпеки охоплюють широкий спектр технологій, які мають забезпечувати цілісність, доступність і конфіденційність даних у різних середовищах, включаючи хмарні технології, мобільні платформи та розподілені мережі. Особливу увагу приділяють захисту інформації у хмарних середовищах, де виникає потреба в нових підходах до забезпечення безпеки через високу доступність даних для

користувачів і динамічні умови зберігання. У результаті комплексна система кіберзахисту сьогодні включає засоби шифрування, автентифікації, контроль доступу, а також інтелектуальні методи виявлення та нейтралізації загроз, що дозволяють адаптуватися до змінюваних умов сучасного кіберсередовища.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Існує велика кількість досліджень у сфері кібербезпеки, що стосуються як програмних, так і апаратних рішень. Розглянуто комплексний підхід до розробки системи захисту, яка використовує методи мультифакторної аутентифікації та динамічний контроль доступу. Загалом потрібно зосереджуватися на питаннях шифрування даних та алгоритмах, що забезпечують більш ефективне шифрування з меншими витратами ресурсів. Згідно з дослідженням , застосування ШІ та машинного навчання дозволяє виявляти аномалії в мережевих трафіках і запобігати більшості атак у режимі реального часу.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою цієї роботи є аналіз технологій підвищення захисту інформації в комп'ютерних мережах та розробка рекомендацій щодо інтеграції сучасних рішень, зокрема, мультифакторної аутентифікації, методів контролю доступу та запобігання загрозам. Стаття також описує вплив використання ШІ та технологій блокчейн для покращення безпеки в хмарних середовищах.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Захист інформації в комп'ютерних мережах сьогодні є одним із найважливіших завдань у сфері кібербезпеки. З розвитком цифрових технологій збільшується ризик кіберзагроз, які можуть призвести до втрати конфіденційної інформації, порушення роботи критичних інфраструктур та значних фінансових втрат. Для забезпечення надійного захисту комп'ютерних мереж розроблено численні технології, кожна з яких має свої переваги та недоліки. До найпоширеніших технологій, що забезпечують кібербезпеку в сучасних мережах, належать мультифакторна аутентифікація, контроль доступу, криптографія, інтелектуальні системи виявлення загроз, апаратні та програмні засоби для захисту мережі, технології блокчейн та хмарні рішення з інтегрованою безпекою.

Мультифакторна аутентифікація (MFA) є важливим компонентом у захисті мереж від несанкціонованого доступу. Традиційна аутентифікація за допомогою лише пароля має значні вразливості, оскільки паролі можуть бути перехоплені або зламані. MFA ж використовує кілька рівнів перевірки, що забезпечує значно вищий рівень захисту. Основні компоненти MFA включають знання (пароль), володіння (мобільний пристрій, на який надсилається код підтвердження), та біометричні фактори (відбиток пальця, розпізнавання обличчя). Наприклад, можна зобразити процес MFA у вигляді діаграми, де кожен етап представляє один із факторів підтвердження.

MFA вимагає інтеграції кількох технологій, що забезпечують одночасно зручність та безпеку. Успішна реалізація цієї технології забезпечує баланс між зручністю використання та захистом, зменшуючи ймовірність того, що зловмисник отримає доступ до мережі навіть у разі компрометації одного з факторів. Наприклад, на етапі біометричної аутентифікації застосовуються технології розпізнавання відбитків пальців або обличчя, а також система безпечного зберігання біометричних шаблонів.

Наприклад:
Псевдокод процесу MFA для авторизації в мережі має наступний вигляд:

```
IF (пароль == вірний) THEN
  Запросити другий фактор аутентифікації (код через SMS чи додаток)
  IF (код == вірний) THEN
    Запросити третій фактор (біометрія)
    IF (біометрія == вірна) THEN
      Доступ надано
    ELSE
      Відмовити в доступі
    ENDIF
  ELSE
    Відмовити в доступі
  ENDIF
ELSE
  Відмовити в доступі
ENDIF
```

Контроль доступу є наступною важливою технологією кібербезпеки. Він забезпечує управління правами доступу до даних та ресурсів мережі на основі ролей та привілеїв користувачів. Система Role-Based Access Control (RBAC) дозволяє адмініструвати права доступу до ресурсів, мінімізуючи ризик

несанкціонованого доступу. Наприклад, у корпоративній мережі права доступу можуть бути розподілені відповідно до посадових обов'язків користувачів, забезпечуючи захист конфіденційних даних. Модель доступу, орієнтована на ролі, може бути представлена діаграмою, де кожна роль має визначений рівень доступу до певних ресурсів.

Для реалізації RBAC застосовуються спеціальні правила, які обмежують дії користувачів на основі їх ролей. Наприклад, псевдокод для надання доступу в системі на основі RBAC виглядає наступним чином:

```
ROLE адміністратора:
  Доступ до всіх ресурсів
ROLE співробітника:
  Доступ до ресурсів рівня співробітника
IF (користувач має роль адміністратора) THEN
  Доступ до всіх ресурсів
ELSE IF (користувач має роль співробітника) THEN
  Доступ до ресурсів рівня співробітника
ELSE
  Відмовити в доступі
ENDIF
```

Криптографія є основою для захисту даних під час їх передачі та зберігання. Алгоритми симетричного шифрування, такі як AES, використовуються для швидкої та ефективної передачі зашифрованих даних. У той же час, асиметричне шифрування, зокрема RSA або ECC, забезпечує високий рівень безпеки для аутентифікації та передачі ключів. Наприклад, шифрування симетричним алгоритмом AES можна представити формулою:

$$C = Ek(M)$$

де C — зашифрований текст, M— початкове повідомлення, E — алгоритм шифрування, а k — ключ. У свою чергу, для асиметричних алгоритмів використовується публічний і приватний ключі для шифрування та розшифрування.

Інтелектуальні системи виявлення та запобігання загрозам (IDS/IPS) забезпечують виявлення аномальних дій у мережевому трафіку та запобігають потенційним загрозам у режимі реального часу. Алгоритми машинного навчання аналізують поведінкові шаблони, що дозволяє виявляти навіть невідомі загрози. IDS та IPS автоматично блокують небезпечний трафік, запобігаючи витоку даних та несанкціонованому доступу. Наприклад, для класифікації трафіку в IDS можна використати алгоритми кластеризації, які дозволяють виявляти аномалії. Функція виявлення аномалій описується так:

$$1, \& \text{якщо } x \text{ — аномалія} \\ 0, \& \text{інакше} \end{cases}$$

де A(x)— функція, що визначає, чи є трафік аномальним (1 — аномалія, 0 — нормальний трафік).

Апаратне та програмне забезпечення для безпеки мережі також є важливим елементом захисту. Апаратні засоби, такі як міжмережеві екрани, шлюзи безпеки та захищені модулі шифрування (HSM), забезпечують додатковий рівень безпеки та можуть інтегруватися з програмними рішеннями. Це дозволяє створити комплексну систему захисту, яка забезпечує більш ефективний захист від кіберзагроз. Наприклад, при використанні VPN забезпечується безпечний тунель для передачі даних, який шифрує інформацію між кінцевими точками.

Технології блокчейн пропонують новий рівень захисту для комп'ютерних мереж, особливо у сфері збереження логів дій та подій. Блокчейн, як незмінний реєстр даних, може використовуватися для безпечного зберігання інформації про доступи, транзакції та дії у мережі, забезпечуючи їхню автентичність і захист від несанкціонованих змін. Це має критичне значення для забезпечення цілісності даних, адже блокчейн дозволяє автоматично фіксувати всі мережеві події та дії користувачів у форматі, який неможливо видалити чи змінити без згоди всіх учасників мережі.

Блокчейн стає потужним інструментом для моніторингу мережевої активності та кіберзахисту. Зберігання даних про доступ та аутентифікацію в блокчейні дозволяє знизити ризик внутрішніх загроз, оскільки жоден користувач не може змінити запис без відповідної верифікації. Це особливо корисно у великих мережах, де потрібно підтримувати надійний контроль доступу та простежувати дії користувачів. Блокчейн допомагає ідентифікувати аномалії та потенційні загрози в режимі реального часу, оскільки всі зміни у мережі відстежуються на блокчейн-рівні, і будь-яка спроба втручання миттєво стає видимою для адміністраторів мережі.

У корпоративних комп'ютерних мережах блокчейн також забезпечує стійкість до зловмисного втручання, особливо при обробці конфіденційних даних. Наприклад, завдяки децентралізованій структурі блокчейну, компанії можуть захистити важливі дані, такі як логи доступів до мережі чи конфігурації систем,

від знищення чи підробки. Децентралізація дозволяє мережам продовжувати працювати навіть у разі часткових атак або збоїв, оскільки інформація зберігається на багатьох вузлах, а не в одному центральному місці.

Інтеграція блокчейн-технологій у комп'ютерні мережі відкриває нові можливості для забезпечення безпеки даних у хмарних середовищах. Для зберігання та передачі інформації в хмарі блокчейн надає додатковий рівень захисту, забезпечуючи незмінність і верифікацію даних без необхідності повністю довіряти стороннім постачальникам хмарних послуг. Блокчейн дозволяє мережевим адміністраторам мати прозорий огляд всіх дій і подій, що відбуваються в хмарних сервісах, підвищуючи загальну безпеку та захист від зовнішніх і внутрішніх кіберзагроз.

Хмарні рішення з інтегрованою безпекою також стають важливою складовою сучасних комп'ютерних мереж. Хмарні провайдери пропонують рішення з інтегрованими інструментами захисту, що включають засоби шифрування, контроль доступу, регулярний аудит та моніторинг загроз. Ці заходи дозволяють зменшити ризики, пов'язані з кібербезпекою у хмарних середовищах. Наприклад, політики безпеки для кожного типу даних можна контролювати на рівні доступу до хмарного середовища, забезпечуючи надійний захист даних у багатокористувацьких платформах.

Перспективи подальших досліджень у сфері кібербезпеки передбачають інтеграцію адаптивних систем захисту, що здатні навчатися на основі нових загроз та автоматично адаптуватися до них. Розвиток технологій штучного інтелекту та розподілених обчислень дозволяє створювати інтегровані рішення, які забезпечують більш ефективний захист комп'ютерних мереж. Іншою важливою областю досліджень є стандартизація протоколів для IoT-пристроїв, що забезпечить ефективне управління та захист інформації у великих мережах, які включають різні пристрої з обмеженими ресурсами.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

З огляду на зростаючу складність кіберзагроз, подальші дослідження повинні зосередитися на розробці адаптивних систем захисту, здатних навчатися та пристосовуватися до нових типів загроз у режимі реального часу. Використання технологій штучного інтелекту (ШІ) та машинного навчання відкриває можливості для створення інтелектуальних систем, які можуть автоматично виявляти та реагувати на аномалії у мережевому трафіку, визначаючи потенційні загрози ще до того, як вони зможуть завдати шкоди. Інтеграція ШІ з блокчейн-технологіями також може забезпечити високий рівень прозорості та надійності, надаючи нові засоби для відстеження та верифікації дій у мережі.

Розвиток розподілених обчислень сприяє створенню ефективних рішень для захисту комп'ютерних мереж, зокрема в умовах розподілених середовищ, таких як хмарні платформи та інфраструктура Інтернету речей (IoT). Подальші дослідження в цій сфері можуть бути спрямовані на розробку архітектур, які дозволять швидко обробляти великі обсяги даних з різних джерел, одночасно забезпечуючи цілісність і конфіденційність інформації навіть при передаванні через незахищені канали.

Ще однією важливою областю досліджень є стандартизація безпекових протоколів для хмарних платформ і IoT-пристроїв. Ці платформи стають усе популярнішими, але залишаються вразливими через відсутність єдиних стандартів захисту. Дані, що передаються через хмарні платформи та IoT-пристрої, часто проходять через загальнодоступні або недостатньо захищені канали, що підвищує ризик перехоплення та несанкціонованого доступу. Впровадження єдиних стандартів для шифрування, автентифікації та контролю доступу в цих системах сприятиме зменшенню вразливостей, підвищенню довіри до таких технологій та покращенню їхньої взаємодії.

Також перспективним напрямом є розробка технологій для підвищення кіберстійкості мереж — здатності швидко відновлюватися після кіберінцидентів і автоматично мінімізувати збитки. Такі системи, що передбачають самовідновлення, можуть мати особливе значення для критичних інфраструктур, де безперебійна робота має вирішальне значення для безпеки та економіки.

Комплексний підхід до захисту інформації, який включає сучасні технології аутентифікації, шифрування, контролю доступу та системи виявлення загроз, є необхідною умовою для забезпечення безпеки у комп'ютерних мережах. Використання ШІ та блокчейну створює додаткові можливості для покращення кіберзахисту, а хмарні рішення з інтегрованими інструментами захисту дозволяють забезпечити високий рівень безпеки у сучасних інфраструктурах. Удосконалення цих технологій відкриває нові перспективи для розробників та дослідників у сфері кібербезпеки.

Література

1. Андрієнко І., Кравчук О. Методи захисту інформації в комп'ютерних мережах / І. Андрієнко, О. Кравчук // Системи захисту інформації. – 2022. – Т. 3. – № 24. – С. 110-120. DOI: https://doi.org/10.20535/1560-8956.24.2022.264104
2. Офіційна документація OpenSSL : [вебсайт]. – Режим доступу : https://www.openssl.org/

3. Романов М.М., Поляков С.В. Криптографія та мережеві протоколи / М.М. Романов, С.В. Поляков // Харків: Харківський національний університет радіоелектроніки. – 2023. – 312 с. – Режим доступу : https://repository.nure.ua/bitstream/123456789/910/1/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf
4. Wireshark: офіційний вебсайт : [вебсайт]. – Режим доступу : https://www.wireshark.org/
5. Metasploit Framework : [вебсайт]. – Режим доступу : https://www.metasploit.com/
6. Nmap: довідка та документація : [вебсайт]. – Режим доступу : https://nmap.org/
7. Snort : [вебсайт]. – Режим доступу : https://www.snort.org/
8. Cisco Security Documentation : [вебсайт]. – Режим доступу : https://www.cisco.com/c/en/us/support/docs/security/
9. OWASP: рекомендації щодо веббезпеки : [вебсайт]. – Режим доступу : https://owasp.org/

References

1. Andriyenko I., Kravchuk O. Information Protection Methods in Computer Networks / I. Andriyenko, O. Kravchuk // Information Security Systems. – 2022. – Vol. 3. – № 24. – P. 110-120. DOI: https://doi.org/10.20535/1560-8956.24.2022.264104
2. Official OpenSSL Documentation : [website]. Access mode : https://www.openssl.org/
3. Romanov M.M., Polyakov S.V. Cryptography and Network Protocols / M.M. Romanov, S.V. Polyakov // Kharkiv: Kharkiv National University of Radioelectronics. – 2023. – 312 p. Access mode : https://repository.nure.ua/bitstream/123456789/910/1/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf
4. Wireshark: Official Website : [website]. Access mode : https://www.wireshark.org/
5. Metasploit Framework : [website]. Access mode : https://www.metasploit.com/
6. Nmap: Documentation and Help : [website]. Access mode : https://nmap.org/
7. Snort : [website]. Access mode : https://www.snort.org/
8. Cisco Security Documentation : [website]. Access mode : https://www.cisco.com/c/en/us/support/docs/security/
9. OWASP: Web Security Guidelines : [website]. Access mode : https://owasp.org/