УДК 004.056:355.451

СТВОРЕННЯ БЕЗПЕЧНИХ ЛОКАЛЬНИХ МЕРЕЖА З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

Тяптя А.В.
Науковий керівник – ст. викл. В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: anastasiia.tiaptia@nure.ua

An analysis of the principles of creating secure local networks using advanced information security technologies was carried out. The key directions in the field of security technologies of local networks are considered. Correct use of encryption technologies, network firewalls, identification and authentication systems, but care must be taken to ensure that the cost of security does not exceed reasonable limits.

У сучасному цифровому світі, де відбувається постійний розвиток технологій, безпека локальних мереж є надзвичайно актуальною проблемою. Зростаюча кількість кіберзагроз та інцидентів з порушенням безпеки мереж підкреслює необхідність удосконалення методів захисту [1].

Мета роботи - дослідження та аналіз принципів створення безпечних локальних мереж з використанням передових технологій інформаційної безпеки.

Зважаючи на швидкі та постійні зміни в кіберзагрозах, розвиток технологій інформаційної безпеки також є невпинним. Ключові напрямки у сфері технологій безпеки локальних мереж:

1. Розширене шифрування даних. Шифрування даних є однією з найважливіших технологій для захисту конфіденційності. Розширені методи шифрування, такі як AES-256, дозволяють забезпечити високий рівень безпеки для пересилання даних через мережу, а також для зберігання інформації на пристроях та серверах [2].

2. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Ці системи виявляють та блокують незвичайну або підозрілу активність у мережі. Вони дозволяють вчасно реагувати на потенційні загрози та вторгнення, запобігаючи їхньому успішному завершенню [3].

3. Методи автентифікації користувачів [4]. Для забезпечення безпеки мережі важливо правильно ідентифікувати та автентифікувати користувачів. Парольні системи, біометричні технології (відбитки пальців, розпізнавання обличчя), а також механізми двофакторної автентифікації надають додатковий рівень безпеки.

4. Інтеграція штучного інтелекту (AI) та машинного навчання (ML). Технології штучного інтелекту та машинного навчання стають все більш важливими в сфері кібербезпеки. Вони дозволяють автоматизувати процес виявлення та аналізу загроз у реальному часі, а також вдосконалювати системи захисту за допомогою аналізу великих обсягів даних.

5. Blockchain технології для захисту даних. Blockchain технології дозволяють створювати розподілені та незмінні записи даних, що робить їх вкрай важливими для забезпечення цілісності та захисту даних у локальних мережах.

Для вирішення вищеназваних проблем існує багато різних способів їх вирішення: використовувати технології AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), SHA (Secure Hash Algorithm), IPsec (Internet Protocol Security).

За допомогою суміщення технологій IDS, IPS та AI можна зробити паралельне машинне навчання та первинну безпеку від вторгнень. Для навчання AI потрібно буде використати достатньо немало коштів, але з часом , для використання його в довгострокову перспективу, кіберзахист буде виконуватись автоматично та реакція між дією та реакцією буде мінімальною. Залишається тільки додати журнал користувачів і щоб AI запам'ятовував їх поведінку.

За допомогою особливостей Blockchain технології - можна створювати розподілену систему записів користвачів. Одним з важливих методів захисту інформації при використанні цієї технології є автоматичне застосування хешування інформації за допомогою хешування. Таким чином ми будемо використовувати найновітніші засоби захисту на базі технологій SHA.

Створення безпечних локальних мереж з використанням передових технологій інформаційної безпеки вимагає системного підходу та поєднання різноманітних заходів захисту [5]. Правильне використання технологій шифрування, мережевих брандмауерів, систем ідентифікації та автентифікації, але треба слідкувати за тим щоб вартість безпеки не перевищувала розумні кордони.

Список використаних джерел

1. Голубничий Д.Ю. et al. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації, 2021.
2. William Stallings. Cryptography and Network Security: Principles and Practice.: Pearson. 2016 p. 752c.
3. Сєвєрінов О.В., Хрєнов А.Г. Аналіз сучасних систем виявлення вторгнень. // Системи обробки інформації 6 (2014): 122-124.
4. Кліпоносова В.С., Сєвєрінов О.В. Сучасні методи біометричної ідентифікації та автентифікації користувачів. // ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.
5. Michael E. Whitman, Herbert J. Mattord. Principles of Information Security. Cengage Learning. 2018 p. 656 c.