УДК 004.056.57

ОЦЕНКА УЯЗВИМОСТЕЙ И УГРОЗ В СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ: МЕТОДЫ ЗАЩИТЫ И ПРЕДОТВРАЩЕНИЯ АТАК

Ализода С.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Лихачевский Д.В. – к. т. н., доцент, декан ФКП

Аннотация. В статье рассматриваются основные угрозы и уязвимости современных компьютерных сетей, включая зловредное ПО, фишинг, DDoS-атаки и социальную инженерию. Также анализируются методы оценки уязвимостей, такие как тестирование на проникновение и аудит безопасности. Описаны ключевые стратегии защиты, включая шифрование, многофакторную аутентификацию и сегментацию сети.

Ключевые слова: кибербезопасность, уязвимости, защита данных, DDoS, фишинг, тестирование на проникновение.

Введение. Современные компьютерные сети являются неотъемлемой частью жизни организаций и частных пользователей. Однако с их развитием увеличивается количество угроз и уязвимостей, которые могут привести к утечке данных, финансовым потерям и сбоям в работе систем. В данной статье рассмотрены основные методы оценки уязвимостей, классификация угроз, а также способы защиты и предотвращения атак.

Основная часть. Методика проведения эксперимента. Современные компьютерные сети подвержены множеству угроз, которые можно классифицировать следующим образом:

1 Зловредное ПО (Malware) – включает вирусы, трояны, черви, ransomware и spyware, которые могут повредить данные или нарушить работу системы. Они могут распространяться через заражённые файлы, электронную почту или вредоносные ссылки.

2 Фишинг (Phishing) – атаки, направленные на получение конфиденциальной информации путём обмана пользователей. Чаще всего реализуются через поддельные веб-сайты или электронные письма, маскирующиеся под легитимные организации.

3 DDoS-атаки (Distributed Denial of Service) – перегрузка сетевых ресурсов с целью отказа в обслуживании. Атакующий использует ботнеты для генерации большого объёма трафика, нарушая работу серверов и сервисов.

4 Атаки на уязвимости программного обеспечения – использование уязвимостей в коде программ с целью получения несанкционированного доступа. Такие атаки включают эксплуатацию переполнения буфера, SQL-инъекции и использование уязвимостей нулевого дня.

5 Социальная инженерия – методы психологического манипулирования с целью получения доступа к защищённым данным. Это может включать подделку личности, манипуляцию через телефонные звонки или электронные письма.

6 Вредоносные инсайдеры – сотрудники или партнеры организации, которые злоупотребляют своим доступом для кражи информации или саботажа системы.

7 Атаки на беспроводные сети – перехват данных в Wi-Fi-сетях через атаки типа «человек посередине» (MITM) или эксплуатацию слабых паролей и незащищённых соединений.

Эффективное управление кибербезопасностью требует регулярного анализа слабых мест в системе. Основные методы оценки уязвимостей включают:

– анализ угроз и рисков – выявление потенциальных угроз и оценка их вероятности и возможного ущерба. Используются методы количественного и качественного анализа рисков;

– тестирование на проникновение (Penetration Testing) – имитация атак для выявления слабых мест в системе. Проводится вручную или с помощью автоматизированных инструментов, таких как Metasploit;

– аудит безопасности – проверка соответствия системы установленным стандартам безопасности, таким как ISO 27001, NIST, PCI DSS;

– мониторинг сетевого трафика – анализ активности в сети для выявления аномального поведения. Используются инструменты, такие как Wireshark и Zeek;

– использование систем управления уязвимостями (Vulnerability Management Systems) – автоматизированные инструменты для поиска и исправления уязвимостей, такие как Nessus, Qualys и OpenVAS;

– ревизия прав доступа – регулярная проверка пользователей и их прав доступа для предотвращения несанкционированного использования информации;

– обнаружение и анализ вредоносного кода – применение sandboxes и поведенческого анализа для выявления неизвестных угроз.

Методы защиты и предотвращения атак. Для обеспечения безопасности компьютерных сетей применяются следующие методы:

1 Шифрование данных – использование криптографических алгоритмов (AES, RSA) для защиты информации от несанкционированного доступа.

2 Многофакторная аутентификация (MFA) – дополнительный уровень защиты учётных записей с использованием одноразовых кодов, биометрии или аппаратных ключей.

3 Межсетевые экраны (Firewall) – фильтрация трафика для предотвращения несанкционированного доступа. Аппаратные и программные межсетевые экраны позволяют блокировать вредоносный трафик.

4 Антивирусное программное обеспечение – выявление и удаление вредоносного ПО, обновление сигнатур угроз.

5 Системы предотвращения вторжений (IPS) и обнаружения атак (IDS) – мониторинг и блокировка подозрительных действий на основе сигнатур и аномалий в трафике.

6 Регулярное обновление программного обеспечения – устранение уязвимостей в операционных системах, приложениях и сетевых устройствах.

7 Обучение сотрудников – повышение осведомлённости о киберугрозах и безопасных методах работы, включая защиту от фишинга и управление паролями.

8 Резервное копирование данных – регулярное создание резервных копий и хранение их в защищённых местах для защиты от ransomware-атак и аппаратных сбоев.

9 Сегментация сети – разделение сети на зоны с разными уровнями доступа для уменьшения риска распространения атак.

10 Мониторинг событий безопасности (SIEM) – системы анализа логов и событий для выявления подозрительной активности и реагирования на инциденты.

Будущее кибербезопасности. С развитием технологий появляются новые угрозы и методы их предотвращения. Основные тенденции в области кибербезопасности включают:

– искусственный интеллект и машинное обучение – использование алгоритмов для выявления угроз в реальном времени;

– квантовая криптография – перспективная технология для обеспечения абсолютной безопасности коммуникаций;

– автоматизация кибербезопасности – внедрение автономных решений для реагирования на инциденты;

– безопасность Интернета вещей (IoT) – разработка стандартов защиты для подключённых устройств.

Заключение. Современные компьютерные сети сталкиваются с множеством угроз, требующих комплексного подхода к защите. Оценка уязвимостей, применение эффективных методов предотвращения атак и постоянное совершенствование систем безопасности позволяют минимизировать риски. Важно учитывать, что безопасность – это не разовое мероприятие, а постоянный процесс, требующий внимания и адаптации к новым угрозам. Использование передовых технологий и стратегий защиты позволит повысить уровень кибербезопасности и снизить вероятность атак.

Список литературы

1. *Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2022.*
2. *Schneier, B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.*
3. *National Institute of Standards and Technology (NIST). Special Publication 800-30: Guide for Conducting Risk Assessments. Gaithersburg, MD: NIST, U.S. Department of Commerce.*
4. *OWASP. OWASP Top Ten Security Risks [Electronic resource]. – Available at: https://owasp.org/www-project-top-ten/. – Accessed: March 20, 2025.*
5. *Cloud Security Alliance. Official Website [Electronic resource]. – Available at: https://cloudsecurityalliance.org. – Accessed: March 20, 2025.*

UDC 004.056.57

ASSESSMENT OF VULNERABILITIES AND THREATS IN MODERN COMPUTER NETWORKS: METHODS OF PROTECTION AND PREVENTION OF ATTACK

Alizoda S.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Likhachevsky D.V. – Cand. Of Sci., Associate Professor, Dean of FCAD

Abstract. The article discusses key threats and vulnerabilities in modern computer networks, including malware, phishing, DDoS attacks, and social engineering. It also analyzes vulnerability assessment methods such as penetration testing and security audits. Key protection strategies such as encryption, multi-factor authentication, and network segmentation are described.

Keywords: cybersecurity, vulnerabilities, data protection, DDoS, phishing, penetration testing.