УДК 004.8

Ализода С.С.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

ЭВОЛЮЦИЯ КИБЕРУГРОЗ: КАК МЕНЯЮТСЯ МЕТОДЫ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

Аннотация. Эволюция киберугроз демонстрирует увеличение сложности и масштабности атак на компьютерные сети. С развитием технологий методы атак также изменяются: от простых вирусов до сложных фишинг-атак и постоянных угроз (*APT*). Работа рассматривает ключевые этапы этой эволюции, классификацию атак и прогнозы для будущего киберугроз.

Ключевые слова: эволюция, киберугрозы, методы атак, компьютерные сети, фишинг, нулевые уязвимости, *APT*, киберпреступность, защита, атаки, уязвимости.

Современный мир все глубже погружается в цифровую реальность, и компьютерные сети стали неотъемлемой частью функционирования не только бизнеса, но и государства, образования, здравоохранения и личной жизни миллионов людей. С увеличением степени цифровизации возрастает и значимость защиты этих сетей от киберугроз, которые за последние десятилетия претерпели колоссальные изменения [1]. От примитивных вирусов и червей прошлого, созданных зачастую ради эксперимента, кибератаки эволюционировали в мощный инструмент шпионажа, саботажа и цифрового вымогательства. В этой статье рассматриваются ключевые этапы трансформации методов атак на компьютерные сети, современные тенденции и наиболее перспективные направления в области защиты.

Кибератаки не всегда были столь сложными и разрушительными, как в наши дни. Их развитие происходило поэтапно, отражая уровень развития цифровых технологий и инфраструктуры. В самом начале основными угрозами были относительно простые вирусы, нередко создававшиеся энтузиастами без злого умысла [2]. Однако уже в начале 2000-х гг. фокус сместился в сторону получения материальной выгоды: появились вредоносные программы, способные красть банковские данные, удаленно управлять устройствами и устанавливать шпионское ПО.

Следующий значительный этап ознаменовался появлением целенаправленных атак, организуемых на основе предварительной разведки и оценки инфраструктуры жертвы. Эти атаки стали основой феномена *APT* (*Advanced Persistent Threat*), где злоумышленники действуют с особой скрытностью, иногда оставаясь в системе в течение месяцев или даже лет, медленно развивая свою атаку [3].

Сегодняшние киберугрозы представляют собой комплексные, многоступенчатые и трудно обнаруживаемые схемы вторжений, часто поддерживаемые на государственном уровне или организованными киберпреступными группами. В частности, заметно усилилось использование методов социальной инженерии [4], при которых злоумышленники манипулируют людьми, чтобы получить доступ к защищенной информации. Эти методы особенно опасны тем, что трудно поддаются техническому контролю и требуют высокого уровня осведомленности со стороны сотрудников организаций.

Все больше атак направлены не на конечного пользователя, а на инфраструктуру, поставщиков и цепочки программного обеспечения [5]. Это позволяет злоумышленникам обойти традиционные средства защиты и получить доступ сразу к множеству целевых систем. Большую угрозу представляют и облачные технологии: ошибки конфигурации, уязвимые *API* и недостаточная изоляция данных становятся уязвимыми точками входа.

В ответ на усложнение атак развиваются и защитные меры, принимающие все более интеллектуальный характер. Одним из наиболее действенных подходов стала архитектура *Zero Trust*, в основе которой лежит отказ от доверия к любым компонентам системы по умолчанию. Такая модель предполагает строгую проверку и верификацию каждого действия, каждого пользователя и каждой машины. Не менее важным элементом современной защиты является поведенческая аналитика, позволяющая не просто выявлять технические сбои, но и анализировать отклонения от нормального поведения пользователей. Это дает возможность обнаруживать внутренние и внешние угрозы на ранних стадиях, до нанесения серьезного ущерба.

Автоматизация реагирования на инциденты также играет ключевую роль в защите. Благодаря системам класса *SOAR* организации могут мгновенно принимать меры по изоляции и нейтрализации угроз без необходимости вмешательства человека. Однако ни одна технология не может быть эффективной без обученного персонала. Образовательные инициативы, направленные на повышение осведомленности сотрудников, становятся таким же важным компонентом киберзащиты, как и технические решения.

Вектор развития киберугроз в будущем, по мнению большинства экспертов, будет направлен в сторону еще более глубокой автоматизации атак, а также их интеграции с информационно-психологическим воздействием [6]. Применение искусственного интеллекта злоумышленниками

позволит проводить высокоточные атаки с учетом поведенческих моделей жертв. Одной из растущих угроз становится распространение синтетических медиа – фальсифицированных изображений, голосов и видеозаписей, которые могут использоваться для компрометации высокопоставленных лиц, шантажа или введения в заблуждение широкой аудитории.

Появление квантовых компьютеров в перспективе может радикально изменить правила игры, разрушив существующие криптографические стандарты. Это требует уже сейчас разработки новых алгоритмов защиты, способных противостоять вычислительным возможностям будущих машин. Также все чаще обсуждаются угрозы, связанные с автономными системами, роботизированными комплексами и цифровыми двойниками, которые при взломе могут стать неконтролируемыми.

Понимание эволюции киберугроз важно не только для специалистов в области информационной безопасности, но и для широкой общественности, поскольку цифровая безопасность – это зона ответственности всех участников цифрового общества. Надежная защита требует не просто технических решений, но и системного подхода к формированию культуры безопасности. Только сочетание технологической, организационной и образовательной составляющих может обеспечить устойчивость к современным и будущим киберугрозам. В условиях непрерывных изменений стратегий атак, единственной стабильной ценностью остается необходимость постоянного развития механизмов защиты.

Список использованных источников:

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.

2. Symantec. Internet Security Threat Report, 2023.

3. FireEye. Threat Intelligence Reports, 2022.

4. Mitnick K. The Art of Deception: Controlling the Human Element of Security. Wiley, 2011.

5. Verizon. Data Breach Investigations Report (DBIR), 2023.

6. Europol. Internet Organised Crime Threat Assessment (IOCTA), 2023.

Alizoda S.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

EVOLUTION OF CYBER THREATS: HOW METHODS OF ATTACKING COMPUTER NETWORKS ARE CHANGING

Abstract. The evolution of cyber threats shows an increase in the complexity and scale of attacks on computer networks. As technology develops, attack methods have shifted from simple viruses to complex phishing attacks and advanced persistent threats (APT). The paper explores key stages of this evolution, attack classification, and forecasts for the future of cyber threats.

Keywords: evolution, cyber threats, attack methods, computer networks, phishing, zero-day vulnerabilities, APT, cybercrime, protection, attacks, vulnerabilities.