УДК 004

Дмитриева М.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

ЭВОЛЮЦИЯ КИБЕРАТАК НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

Аннотация. В статье рассматривается эволюция кибератак на критическую информационную инфраструктуру, а также актуальные угрозы и уязвимости информационной безопасности. Особое внимание уделено способам и средствам защиты от кибератак на объекты критической инфраструктуры в связи с инновациями в кибербезопасности.

Ключевые слова: нформационная безопасность, защита информации, кибератака, критическая инфраструктура, кибербезопасность.

В современных реалиях кибератаки на критическую информационную инфраструктуру (КИИ) происходят все чаще и при этом приводят к более разрушительным последствиям. Они представляют угрозу для энергетики, транспорта, здравоохранения, а также для финансового сектора. Для оптимальной защиты КИИ только технологических решений недостаточно, чтобы отразить атаки злоумышленников на критически важную инфраструктуру. Необходим всесторонний инновационный подход, включающий в себя не только современные инструменты, но и квалифицированный персонал, оптимизированные процессы и передовые стратегии развития.

До 2010 г. кибератаки на КИИ носили в основном экспериментальный характер и редко приводили к масштабным последствиям. Примером является атака вируса Stuxnet в 2010 г., направленная на иранские ядерные объекты, что продемонстрировало возможность использования цифровых атак для разрушения физических объектов.

В период с 2010 по 2020 г. наблюдался рост атак на промышленные и энергетические системы. Среди важных инцидентов можно выделить следующие:

– 2015 г. – атака BlackEnergy на энергосистему Украины, вызвавшая массовые отключения электричества;

– 2017 г. – атака вируса NotPetya, поразившего финансовые и государственные системы Украины, а затем распространившегося по всему миру;

– 2020 г. – взлом SolarWinds, затронувший правительственные и корпоративные сети США.

В последние годы кибератаки используются наравне с традиционными военными, экономическими и информационными методами ведения конфликтов. Это значит, что государства и злоумышленники активно применяют цифровые атаки для достижения стратегических политических и экономических целей. По данным компании KnowBe4, специализирующейся на кибербезопасности, во всем мире количество таких атак увеличилось на 30 % с 2022 г., достигнув более 420 млн атак в период с января 2023 по 2024 г., что эквивалентно 13 атакам в секунду. Крупнейшими инцидентами стали:

– 2022–2024 гг. – рост атак на транспортные системы и аэропорты (кибератака на лондонский Heathrow в 2023 г.);

– 2024 г. – США и союзные страны обвинили Россию в использовании вредоносного ПО WhisperGate для атак на Украину и НАТО.

В январе 2025 г. эксперты «Лаборатории Касперского» сообщили о росте количества целевых кибератак на промышленные предприятия в России. Так, по сравнению с предыдущим годом количество атак выросло в 2,5 раза и составило порядка 130 000 инцидентов, из которых критичными стали порядка 25 000. Чаще всего вредоносные объекты проникают на компьютеры автоматизированных систем управления из интернета. Доля утечек из серверов баз данных в общем числе составила 68 %. Кроме того, к кибератакам на объекты КИИ подключились различные группы хактивистов, начав активно атаковать компании, относящиеся к важным секторам экономики с позиции обеспечения национальной безопасности. Причиной стало недостаточное внимание разработчиков, администраторов и архитекторов баз к безопасности, наличие уязвимостей в используемых продуктах и решениях, а также неправильная конфигурация.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций уделяет приоритетное внимание укреплению защиты от киберугроз на территории России. В соответствии со своими функциями, в 2024 г. Роскомнадзор заблокировал доступ к 7724 мошенническим веб-страницам и прекратил деятельность 62 сайтов, занимавшихся распространением вредоносного софта. Все эти действия направлены на обеспечение безопасности КИИ от киберпреступлений, которые приобретают все более сложный и угрожающий характер. Принимаемые меры позволяют снизить риски и предотвратить возможный ущерб от действий злоумышленников в цифровой среде, поскольку успешная атака может привести к безвозвратной утрате данных и неприемлемым последствиям, таким как падение производственной эффективности. В свою очередь, злоумышленники также применяют ИИ для создания вредоносных инструментов и улучшения техник атак с использованием социальной инженерии.

Стоит отметить, в последнее время промышленные организации для увеличения продуктивности, активно внедряют передовые технологии:

искусственный интеллект (ИИ), машинное обучение, дополненную реальность и другие. Внедрение ИИ для улучшения управления производственными процессами уже демонстрирует значительные выгоды в различных отраслях: автоматизированное управление уменьшает риски поломок и остановок в работе, повышая тем самым производительность устройств. В связи с этим, подобные системы стремительно превращаются в критически важные производственные ресурсы, однако их применение также влечет за собой новые риски в области кибербезопасности. Неправильное использование искусственного интеллекта может спровоцировать случайную утечку информации и другие угрозы, многие из которых сложно предвидеть.

В связи с политикой импортозамещения в РФ, для субъектов критической информационной инфраструктуры (КИИ) приоритетным является использование отечественных средств защиты. В частности, для предотвращения несанкционированного доступа (НСД) рекомендуется применять разработки компаний «Код Безопасности», «Инфотекс» и «Конфидент». Для управления информационной безопасностью, оперативного реагирования на инциденты (SIEM) и контроля технологического трафика (INAD) эффективны решения от «Positive Technologies» и «Лаборатории Касперского». Защиту каналов связи (NGFW/VPN) целесообразно обеспечивать продуктами «UserGate», «Кода Безопасности», «Инфотекс», «КриптоПро» и «С-терра». В сфере промышленных межсетевых экранов, востребованными для защиты КИИ являются решения «UserGate» и «Инфотекс», а для управления уязвимостями – продукты «Positive Technologies» и «Алтэкс-Софт».

Надежная защита данных, безопасность ИТ-инфраструктуры, в том числе объектов КИИ, сохранение штатного функционирования бизнес-процессов и соблюдение требований законодательства – обязательные условия устойчивого развития современного бизнеса. Отечественные разработчики представляют для субъектов КИИ готовые решения, которые позволяют создать комплексную систему защиты, позволяющую обеспечить требуемый уровень информационной безопасности.

Список использованных источников:

1. Егорова А.О. Обеспечение безопасности критической информационной инфраструктуры: учебное пособие / сост. А.О. Егорова [и др.]. Севастополь: СевГУ, 2024. 110 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/450542 (дата обращения: 06.04.2025). URL: для авториз. пользователей.

2. Корниенко А.А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры: учебное пособие / А.А. Корниенко, В.С., А.П. Глухов. Санкт-Петербург: ПГУПС, 2022. 63 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/

book/329477 (дата обращения: 06.04.2025). URL: для авториз. пользователей.

3. Середкин С. П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. 2022. № 4 (16). С. 56–66.

4. Лаборатория Касперского, «Лаборатория Касперского» представила прогноз развития сложных кибератак в 2025 г. // kaspersky.ru. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-predstavila-prognoz-razvitiya-slozhnyh-kiberatak-v-2025-godu.

Dmitrieva M.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

THE EVOLUTION OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Abstract. The article examines the evolution of cyberattacks on critical information infrastructure, as well as current threats and vulnerabilities to information security. Special attention is paid to ways and means of protection against cyberattacks on critical infrastructure facilities in connection with innovations in cybersecurity.

Keywords: information security, information security, cyberattack, critical infrastructure, cybersecurity.