УДК 003

Биктубаева К.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. Обеспечение информационной безопасности на объектах критической информационной инфраструктуры является одной из приоритетных задач государственных и частных организаций. Статья посвящена ключевым угрозам безопасности объектов критической информационной инфраструктуры. Особое внимание уделяется комплексной защите, сочетающей организационные, правовые, программные, аппаратные и технические меры защиты.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, защита информации, комплексная защита, угроза.

В условиях цифровизации обеспечение защиты объектов критической информационной инфраструктуры (КИИ) приобретает особую значимость. К ним относятся: информационные системы, информационно-телекоммуникационные сети, автоматизированные систему управления КИИ. Они являются важным элементом, которые поддерживают работу государства и бизнеса. Их защита требует комплексного подхода, включающего все средства защиты информации.

В соответствии с Федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ), под КИИ понимается, объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов [1]. Значимый объект критической информационной инфраструктуры (КИИ) – это объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ.

Кибератаки на объекты КИИ представляют потенциальную угрозу и могут принимать различные формы. По данным исследований на 2024 г., отмечается рост сложности атак на 37 % по сравнению с предыдущим периодом. Согласно статистическим данным экспертов Anti-Malware, объекты КИИ подвергаются рискам трех типов: техническим, эксплуатационным и организационным. Каждый из этих факторов

представляет серьезную опасность для защиты критически важных объектов. Распространенные угрозы:

1. Наибольшую угрозу представляют несанкционированное получение доступа к защищаемой информации, которое может быть совершено как внешними злоумышленниками, так и инсайдером.

2. Опасность несут вирусные атаки с требованием выкупа, когда критически важная информация подвергается шифрованию с последующим шантажом. В 2024 г. наибольшую активность демонстрируют атаки с применением шифровальщиков. 51 % инцидентов в сегменте КИИ за второй квартал 2024 г. были связаны именно с этим типом вредоносного ПО [2].

3. Согласно данным НКЦКИ, распределенные атаки на отказ в обслуживании занимают значительную долю (16 % в 2023 г.) среди угроз, направленных на КИИ. Эти атаки входят в тройку самых распространенных наравне с вирусными программами и ошибками персонала [3].

4. Особое место занимают методы социальной инженерии. Фишинг и целевые рассылки с опасными вложениями сталь настолько изощренными, что 73 % успешных проникновений в систему КИИ начинаются именно с компрометации учетных данных через психологическое воздействие. Даже сложные многоступенчатые атаки начинаются с хищения учетных данных через методы социального воздействия.

Для эффективного противодействия современным угрозам безопасности объектов КИИ необходимо внедрение комплексной системы защиты, включая организационно-правовые, программно-аппаратные и технические меры [4].

Правовые меры составляют основу обеспечения безопасности объектов КИИ. Обязательным требованием является соблюдение положений ФЗ № 187 и соответствующих нормативных актов ФСТЭК № 235, 236, 239 и ФСБ России. Важном элементом правой защиты становится включение объектов в Реестр КИИ и полноценная реализация требований Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), являющаяся подразделением ФСТЭК, а также требований Национального координационного центра по компьютерным инцидентам (НКЦКИ), которая является подразделением ФСБ России [5]. Дополнительно каждая организация должна разрабатывать собственные нормативные документы, регламентирующие порядок обработки и защиты информации.

Технические меры защиты претерпевают значительные изменения благодаря внедрению инноваций. Перспективными направлениями являются системы на базе искусственного интеллекта (ИИ) для обнаружения аномалий, использование квантовой криптографии и развертывание облачных платформ безопасности с автоматическим реагированием [6].

Организационные меры включают три основных направления: регулярный аудит безопасности для выявления уязвимостей в системах, внедрение модели разграничения доступа с применением принципа

минимальных привилегий и многофакторной аутентификации, а также систематическое обучение персонала [7].

К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры, относятся система защиты от несанкционированного доступа, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусы, SIEM-системы, регулярное резервное копирование, обновление ПО и использование защищенных каналов связи [8], [9].

Кибератаки на КИИ прогрессируют, начиная от самых простых вирусов до сложных многоступенчатых атак. Эффективная защита объектов КИИ в современных условиях требует перехода от традиционных методов к адаптивным системам безопасности [10]. Реализация угроз может привести к прекращению или нарушению нормального функционирования значимого объекта, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации). Законодательство дает основную базу для защиты, но без комплексного использования средств защиты, обеспечить полную защиту невозможно. Обеспечение безопасности значимого объекта достигается путем принятия в рамках подсистемы безопасности значимого объекта совокупности организационных, программно-аппаратных и технических мер, направленных на нейтрализацию угроз безопасности информации. Для снижения рисков КИИ необходимо проводить регулярный аудит, который помогает оценить текущий уровень защиты, проанализировать угрозы и принять ряд мер по повышению эффективности защиты системы.

Список использованных источников:

1. Федеральный законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=43150#OU7AUhUSG1BHGtM81/ (дата обращения: 10.04.2025).

2. Аналитический отчет Anti-Malware.ru «Безопасность КИИ: итоги 2024 г. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/CII-security-AMLive-2024. (дата обращения: 10.04.2025).

3. Отчет НКЦКИ за 2023 г. «Анализ киберугроз для объектов КИИ». URL: https://www.cert.gov.ru / (дата обращения: 10.04.2025).

4. Обеспечение защиты и безопасности объектов КИИ. URL: https://rtmtech.ru/articles/obespechenie-zashhity-i-bezopasnosti-obektov-kii /. (дата обращения: 10.04.2025).

5. Защита значимых объектов критической информационной инфраструктуры / URL: https://is.astral.ru/news/blog/zashchita-znachimykh-obektov-kriticheskoy-informatsionnoy-infrastruktury/ (дата обращения: 10.04.2025).

6. Изменения в работе с критической информационной инфраструктурой. URL: https://securitymedia.org/info/izmeneniya-v-rabote-s-kriticheskoy-informatsionnoy-infrastrukturoy-kii-v-2022-godu.html/ (дата обращения: 10.04.2025).

7. Методические рекомендации по обеспечению безопасности критической информационной инфраструктуры. URL: https://aciso.ru/files/docs/metodichka_2.0.pdf (дата обращения: 10.04.2025).

8. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

9. Андреев, М.Ф. Обработка сетевых пакетов в ядре Linux для противодействия атакам типа «отказ в обслуживании» / М.Ф. Андреев, А.С. Исмагилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 г. Уфа: Уфимский университет науки и технологий, 2023. С. 9–14.

10. Исмагилова, А.С. Теоретико-графовая интерпретация системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 9(117). С. 171–179.

Biktubayeva K.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF ENSURING INFORMATION SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Abstract. The article is devoted to the key security threats to critical information infrastructure facilities. Special attention is paid to comprehensive protection, combining organizational, legal, software, hardware and technical protection measures.

Keywords: critical information infrastructure, information security, data protection, complex protection, threat.