Инженерный вестник Дона, №4 (2024)
ivdon.ru/ru/magazine/archive/n4y2024/9176

Разработка концепции обеспечения безопасности критической информационной инфраструктуры финансового сектора

С.А. Корчагин, Д.В. Сердечный, Е.С. Раздьяконов, Беспалова Н.В.

Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: Работа посвящена разработке концепции обеспечения безопасности для защиты критической информационной инфраструктуры финансового сектора. Проведен анализ критической информационной инфраструктуры финансового сектора, рассмотрены основные виды кибератак применительно к объектам в данной области. Предложена концепция безопасности, включающая управление доступом, многоуровневую защиту, шифрование данных, непрерывный мониторинг и другие меры. Приводятся модели основных угроз безопасности объектов информационной инфраструктуры финансового сектора. Поднимается вопрос о значимости сотрудничества и обмена информацией между финансовыми институтами, регулирующими органами и правоохранительными органами для обеспечения коллективной безопасности финансового сектора. Статья будет полезна для специалистов в области информационной безопасности, финансового сектора и руководителей организаций, заинтересованных в разработке и улучшении системы безопасности информационной инфраструктуры предприятия.
Ключевые слова: информационная безопасность, информационная инфраструктура, финансовый сектор, математическое моделирование, программный комплекс.

Введение

Финансовая система является квинтэссенцией функционирования экономики страны [1]. Современная финансовая система включает в себя множество элементов, которые взаимосвязаны между собой с использованием современных коммутационно-информационных технологий. Таким образом, на сегодняшний день, финансовый сектор стал полностью зависим от компьютерных систем, которые играют важную роль в обработке [2,3], хранении [4,5] и передаче большого объема конфиденциальных данных [6,7]. Однако, с развитием технологий и увеличением охвата населения доступом к сети Интернет, возникают все более сложные угрозы безопасности, которые могут повлечь серьезные последствия для финансовой системы.

Цель исследования - разработка концепции обеспечения безопасности критической информационной инфраструктуры (КИИ) финансового сектора. В работе рассматривается аспекты безопасности в указанном секторе, а также

основные угрозы, с которыми сталкиваются пользователи информационной инфраструктуры. В ходе исследования предложены ключевые принципы и меры для защиты информационной инфраструктуры и критически важных элементов финансового сектора от возможных атак и инцидентов безопасности.

Анализ угроз безопасности критической информационной инфраструктуры финансового сектора

КИИ финансового сектора является объектом повышенного внимания для злоумышленников из-за ее важности и значимости для экономики и финансовой стабильности. В работе проведено исследование основных угроз безопасности КИИ финансового сектора России. Основные угрозы безопасности, с которыми сталкивается критическая информационная инфраструктура финансового сектора, можно разделить на несколько основных групп: кибератаки, внутренние угрозы, системные уязвимости, социальная инженерия, законодательные и регуляторные требования. На рисунке 1 приводится распределение угроз безопасности КИИ финансового сектора в Российской Федерации на 2024 г. Для анализа использовались открытые данные, включая данные Центрального банка Российской Федерации [8], Министерства внутренних дел Российской Федерации [9], а также данные Федеральной службы государственной статистики [10]. Рассмотрим каждый вид угроз более подробно. К основным видам кибератак относятся: DDoS-атаки, фишинг и фарминг, мошенничество с карточками. Злоумышленники могут использовать DDoS-атаки для перегрузки серверов и сетей, что приводит к временной недоступности онлайн-банковских услуг и торговых платформ. Атаки через фишинговые письма и веб-сайты могут использоваться для кражи личной информации клиентов, такой, как учетные данные для входа в банковские системы. Взломанные базы данных могут

быть использованы для кражи информации о платежных картах и последующего мошенничества с использованием этих данных.

Рис. 1. – Угрозы безопасности КИИ финансового сектора в Российской Федерации на 2024 г.

К основным внутренним угрозам относятся: утечка данных, а также несанкционированный доступ к данным. Сотрудники финансовых учреждений могут находиться под воздействием социальной инженерии и действовать в целях злоумышленников, в результате чего конфиденциальная информация может быть скомпрометирована. Мошенники используют уязвимости информационных систем и получают доступ к данным финансовых учреждений, чтобы совершить кражу. Важным аспектом угроз безопасности КИИ финансового сектора являются системные уязвимости, к которым относятся отсутствие своевременной установки обновлений программного обеспечения и сложность архитектур информационных

систем. Пренебрежение установкой критически важных обновлений программного обеспечения существенно повышает риск противодействия уязвимостям, которые могут быть использованы злоумышленниками для взлома систем и сетей. Крупные финансовые институты часто имеют сложные архитектуры систем, что может повысить вероятность наличия уязвимостей. Еще одной существенной угрозой безопасности КИИ финансового сектора является социальная инженерия. Социальная инженерия - это метод манипулирования людьми с целью получения конфиденциальной информации или выполнения определенных действий. Данный метод часто используется хакерами и мошенниками для доступа к защищенным данным или получения финансовой выгоды. Примеры социальной инженерии включают в себя звонки или электронные письма от лиц, выдающих себя за представителей банков, компаний или государственных учреждений, с просьбой предоставить личные данные или пароли. Также это может быть использование манипулятивных психологических техник для того, чтобы убедить человека выполнить определенные действия, например, открыть вредоносную ссылку или приложение. Нарушение законодательных и регуляторных требований является также существенной угрозой безопасности КИИ финансового сектора. Финансовые учреждения должны в строгом порядке соблюдать законодательство и регуляторные требования по обеспечению безопасности и конфиденциальности данных клиентов, нарушения этих требований может также создавать существенные угрозы КИИ.

Концепция безопасности критической информационной инфраструктуры финансового сектора

В рамках исследования разработана концепция безопасности КИИ в финансовом секторе. Концепция включает в себя следующие основные элементы:

1. Создание комплексной системы защиты КИИ. Комплексная система должна включать в себя физические, логические и криптографические меры безопасности. К физическим мерам относится установка безопасности на входах, видеонаблюдение, контроль доступа и д.р. Логические меры могут включать в себя использование брандмауэров, систем обнаружения вторжений и систем мониторинга. Криптографические меры предполагают шифрование данных, использование электронных подписей и пр.

2. Разработка политики информационной безопасности. Политика информационной безопасности определяет правила и процедуры. К ним относятся требования к сложности паролей, ограничение доступа к конфиденциальной информации, регулярное обновление программного обеспечения.

3. Периодический аудит безопасности КИИ. Для поддержания высокого уровня безопасности КИИ, компании финансового сектора должны проводить регулярный аудит безопасности и проверку систем на уязвимости. Аудит включает в себя сканирование сети, проверку безопасности веб-приложений, проверку соответствия политике безопасности. Выявленные проблемы безопасности должны быть немедленно устранены.

4. Обучение сотрудников. Сотрудники финансового сектора должны быть обучены правилам безопасности и знать, как правильно обращаться с конфиденциальной информацией, как распознать и предотвратить фишинговые атаки, а также как реагировать на инциденты, связанные с социальной инженерией. Обучение должно проводиться регулярно,

поскольку новые угрозы появляются постоянно, а методы защиты быстро устаревают.

5. Сотрудничество с ведущими поставщиками решений в области информационной безопасности. Сотрудничество компаний финансового сектора с ведущими поставщиками продуктов в области информационной безопасности позволит обеспечить наилучшими технологиями защиты КИИ. Ведущие поставщики предоставляют профессиональные услуги в области информационной безопасности, поддерживают регулярные обновления и предупреждают о новых угрозах и сбоях.

6. Соблюдение нормативов и требований. Это включает в себя требования ФСТЭК, ФСБ, стандарты информационной безопасности и пр.

Внедрение данных мероприятий может в существенной мере повысить защищенность КИИ в финансовом секторе и снизить риск различных видов атак и утечек информации.

В ходе исследования был проведен анализ 32 компаний финансового сектора. Использовались статистические данные, в целях соблюдения политики конфиденциальности, данные о компаниях были обезличены. Компаниям был предоставлен чек-лист предложенной концепции безопасности. На рисунке 2, показаны диаграммы, на которых изображены усредненные значения частоты угроз и уязвимостей по исследуемым компаниям: было (если не выполняется хотя бы один пункт из предложенной концепции) и стало (при условии выполнении всех пунктов концепции безопасности КИИ). Как видно из рисунка, даже на небольшом количестве компаний, принявших участие в эксперименте, наблюдается существенный положительный эффект от внедрения данной концепции.

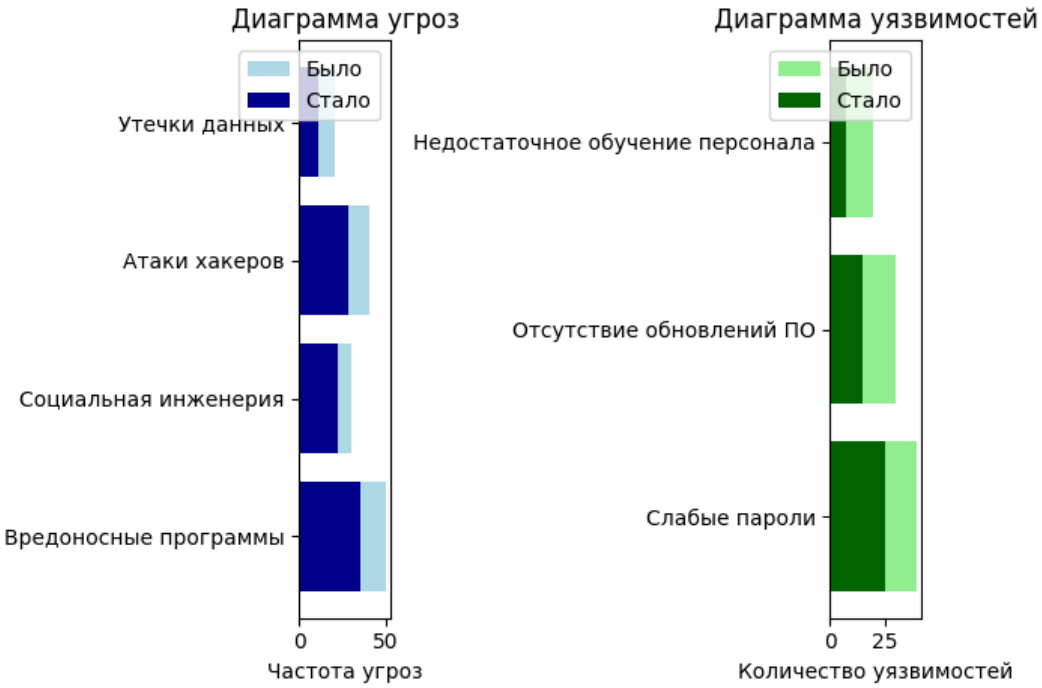

Рис. 2. – Усредненные значения частоты угроз и уязвимостей (до внедрения концепции безопасности КИИ и после внедрения)

Заключение

В работе рассмотрена актуальная проблема обеспечения безопасности критической информационной инфраструктуры финансового сектора. С учетом стремительного развития информационных технологий и увеличения числа киберугроз стало очевидным, что безопасность информационных систем является одним из ключевых аспектов в обеспечении стабильности финансового сектора.

В ходе исследования была разработана концепция обеспечения безопасности критической информационной инфраструктуры финансового сектора, которая включает в себя комплекс мер и механизмов защиты от различных угроз и уязвимостей. В основе этой концепции лежит системный подход, который учитывает, как технические, так и организационные аспекты безопасности. Полученные результаты будут полезны специалистам

по информационной безопасности, системным администраторам, инженерам по сетям и другим ИТ-специалистам, которые ответственны за обеспечение безопасности информационных систем, финансовым аналитикам и консультантам, для лучшего понимания рисков, связанных с безопасностью КИИ, а также регуляторным органам и законодателям при разработке политики и законодательства в области информационной безопасности в финансовом секторе.

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета

Литература

1. Колмыкова Т.С., Клыкова С.В. Роль цифровых финансовых сервисов и технологий в развитии современной архитектуры экономического пространства //Регион: системы, экономика, управление. – 2021. – №. 2 (53). – С. 11-17.

2. Abrahams, Temitayo & Ewuga, Sarah & Kaggwa, Simon & Uwaoma, Prisca & Hassan, Azeez & Dawodu, Samuel. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews. 20. 1743-1756. 10.30574/wjarr.2023.20.3.2691.

3. Корчагин С.А., Догадина Е.П., Мелентьев В.В., Никитин П.В., Сердечный Д.В. Автоматизированная система выдачи банковских гарантий на основе прогнозирования исполнения государственных контрактов //Инженерный вестник Дона, 2023, №. 8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8600

4. Kafi M. A., Akter N. Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection //American Journal of Trade and Policy. – 2023. – Vol. 10. – No. 1. – pp. 15-26.

5. Ибрагимова З. М., Батчаева З. Б., Ткаченко А. Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона. 2022. №. 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

6. Феклин В.Г. Соловьев В.И., Корчагин С.А., Царегородцев А.В. Методы машинного обучения в задачах контроля криптовалютных транзакций // Вопросы кибербезопасности. – 2023. – №. 4. – С. 2-11.

7. Javaid M. et al. A review of Blockchain Technology applications for financial services // BenchCouncil Transactions on Benchmarks, Standards and Evaluations. – 2022. – Vol. 2. – No. 3. – p. 100073.

8. Гондарь В. В., Зиниша О. С., Шаронова В. А. Политика Банка России по обеспечению кибербезопасности в банковской сфере // Современные научные исследования и разработки. – 2018. – Т. 1. – №. 12. – С. 179-183.

9. Комаревцева И. В. Основные направления участия органов внутренних дел в системе кибербезопасности // Образование и право. – 2022. – №. 11. – С. 189-191.

10. Мещерякова Ж. В. Федеральные статистические наблюдения и международные стандарты: проблемы гармонизации //Актуальные проблемы и перспективы развития государственной статистики в современных условиях. – 2019. – С. 139-142.

References

1. Kolmykova T.S., Klykova S.V. Region: sistemy, ehkonomika, upravlenie. 2021. №. 2 (53). p. 11-17.

2. Abrahams T., Ewuga S., Kaggwa S., Uwaoma P., Hassan A., Dawodu S. World Journal of Advanced Research and Reviews, 2023, №. 20, p. 1743-1756. DOI 10.30574/wjarr.2023.20.3.2691.

3. Korchagin S.A., Dogadina E.P., Melent'ev V.V., Nikitin P.V., Serdechnyi D.V. Inzhenernyj vestnik Dona, 2023, №. 8. URL: ivdon.ru/ru/magazine/archive/n8y2023/8600

4. Kafi M. A., Akter N. American Journal of Trade and Policy. 2023. Vol. 10. №. 1. p. 15-26.

5. Ibragimova Z.M., Batchaeva Z.B., Tkachenko A.L. Inzhenernyj vestnik Dona. 2022. №. 11. URL: ivdon.ru/ru/magazine/archive/n11y2022/8010

6. Feklin V.G. Solov'ev V.I., Korchagin S.A., Tsaregorodtsev A.V. Voprosy kiberbezopasnosti. 2023. №. 4. p. 2-11.

7. Javaid M. et al. BenchCouncil Transactions on Benchmarks, Standards and Evaluations. 2022. Vol. 2. №. 3. p. 100073.

8. Gondar V. V., Zinisha O. S., Sharonova V. A. Sovremennyye nauchnyye issledovaniya i razrabotki. 2018. Vol. 1. №. 12. p. 179-183.

9. Komarevtseva I. V. Obrazovaniye i pravo. 2022. №. 11. S. 189-191.

10. Meshcheryakova Zh. V. Aktualnyye problemy i perspektivy razvitiya gosudarstvennoy statistiki v sovremennykh usloviyakh. 2019. p. 139-142.

Дата поступления: 12.03.2024

Дата публикации: 19.04.2024