

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ FINTECH

Фролова М.И. (ИТМО)

Научный руководитель – к.э.н., доцент Гаврилюк Е.С. Университет ИТМО
(ИТМО)

В данном докладе исследуются риски информационной безопасности в сфере финтех.

Введение. FinTech является перспективной сферой развития финансового сектора, активно конкурирующей с устоявшимися финансовыми организациями. Согласно определению Центрального банка РФ финтех (финансовые технологии) – это предоставление финансовых услуг и сервисов с использованием инновационных технологий, таких как «большие данные» (Big Data), искусственный интеллект и машинное обучение, роботизация, блокчейн, облачные технологии, биометрия и других [1].

Финтех организации оперируют в своей деятельности персональными и финансовыми данными пользователей. Угрозы конфиденциальности, целостности и доступности данных этих категорий могут повлечь такие последствия, как экономические потери для пользователей и организации, кражу цифрового портрета пользователей, а также репутационный ущерб организации, ведущий к обесцениванию акций и последующему банкротству.

Исследование основных угроз информационной безопасности для финтех-организаций позволит избежать их на этапе проектирования системы и поспособствует оптимальному распределению ресурсов на этапе поддержания системы.

Основная часть.

При анализе научной литературы были выявлены следующие основные угрозы информационной безопасности финтех-организаций [2]:

- Утечки данных;
- Социальный инжиниринг;
- Вирусные атаки;
- DDOS атаки;
- Внутренние атаки.

Исследование угроз за 2020 год показало, что наибольшее количество угроз с высокой стоимостью приходится на категории утечек информации, вирусные атаки и социальный инжиниринг, а именно фишинговые атаки. [3]

Количество инцидентов, связанных с утечками информации составило 800 случаев, стоимость оценена в 12.5 млн. долларов.

Количество инцидентов, связанных с фишинговыми атаками, составило 200 случаев, стоимость оценена в 8.2 млн. долларов.

Количество инцидентов, связанных с вирусами, составило 400 случаев, стоимость оценена в 15.7 млн. долларов.

Все выделенные угрозы напрямую влияют на сохранность данных пользователей и организации.

После рассмотрения основных типов угроз информационной безопасности в финтех-организациях целесообразно рассмотреть, какие последствия имеют успешные атаки.

Финансовый сектор является наиболее уязвимым по отношению к кибер-атакам из-за ценности обрабатываемых данных. Эксперты Банка России указывают, что до 17% всех кибер-атак приходится на финансовый сектор. Финтех-организации как представители сектора с высокой степенью цифровизации являются самой вероятной целью злоумышленников. Ежегодные потери для России ежегодно достигают 600 млрд рублей. [4]

Помимо финансовых рисков следует также учитывать репутационные потери для организации. В случае успешной атаки пользователи продукта финтех-организации менее склонны доверять как конкретной организации, так и сектору финтеха в целом. Крупные

атаки также могут привести к неблагоприятным изменениям на фондовом рынке.

Выводы. Проведен анализ вероятности возникновения и экономической значимости угроз информационной безопасности в сфере FinTech. Анализ показал приоритет финансового сектора в кибер-атаках, а также высокую стоимость успешных атак.

Список использованных источников:

1. Развитие финансовых технологий // Центральный банк РФ: обзор. 2024.. URL: <https://cbr.ru/fintech/> (дата обращения 18.02.2025);
2. Danial Javaheri, Mahdi Fahmideh, Hassan Chizari, Pooia Lalbakhsh, Junbeom Hur Cybersecurity threats in FinTech: A systematic review // Expert Systems with Applications – 2023. – № 241;
3. Paulin K. Kamuangu A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends // Journal of Economics, Finance and Accounting Studies – 2024. – С. 47-53;
4. Семеко Галина Викторовна Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки – 2020. – №1. – С. 77-96.