Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Современные технологии в сфере обеспечения финансовой безопасности российских банков

Научный руководитель – Хабибулин Алик Галимзянович

Абакарова Амина Мурадовна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: amina.abackarova@yandex.ru

Финансовая безопасность является актуальной проблемой для современных государств и для общества в целом. С ростом использования интернета и цифровизацией общества угрозы в онлайн-пространстве и финансовой среде продолжают увеличиваться. Рядовые граждане – не единственные, кто может подвергаться рискам. Банки также становятся целями массивных кибератак, что определяет необходимость разработки современных технологий, способных предотвратить киберпреступления в сфере финансовой безопасности банков.

Глобальный ущерб от киберпреступности оценивается в 8 трлн. долларов за период с 2018 по 2022 гг. К 2025 г. по оценкам экспертов потери в интернет-сегменте вырастут до 11 трлн дол., а к 2030 г. киберугрозы смогут нанести еще больший урон экономике – около 90 трлн дол., что говорит о негативной экспоненте (Лавров, 2020). Риск киберпреступности растет с каждым годом, и он затрагивает компании любого размера. Малые компании более уязвимы к кибератакам, а стоимость инцидентов на одного сотрудника у небольших компаний выше, чем у крупных.

Финансовая безопасность российских банков претерпевает радикальные изменения под влиянием технологических инноваций и усиления регуляторного контроля. В 2024-2025 годах отрасль демонстрирует беспрецедентный рост инвестиций в кибербезопасность (на 30-60% по сравнению с 2023 годом), активное внедрение отечественных решений и переход к проактивным моделям защиты. Ключевыми драйверами преобразований стали новые стандарты Центробанка для открытых API, платформа «Прозрачный блокчейн» Росфинмониторинга и интеграция искусственного интеллекта в системы обнаружения угроз. При этом сохраняются вызовы, связанные с усложнением методов социальной инженерии и атаками через цепочки поставок.

Финансовая безопасность кредитной организации представляет собой систему мероприятий, которая способствует стабильному функционированию банка, предотвращению внутренних и внешних угроз. Система финансовой безопасности должна быть уникальной в каждом банке, поскольку зависит от направления деятельности банка, продажи соответствующих банковских продуктов и услуг для отдельных потребителей. Только комплексность на согласованность системы финансовой безопасности банка может обеспечить надежность его безопасности (Васильева Ю.А., 2023, с.67).

Одной из проблем обеспечения финансовой безопасности является телефонное мошенничество. Мошенники используют приемы социальной инженерии, чтобы обмануть своих жертв, и часто выдавая себя за сотрудников правоохранительных органов, Центрального банка РФ, службы безопасности банков и т.д. Судя по последним данные телефонное мошенничество приобрело масштабы национального бедствия, и мошенники ежедневно совершают более 8,5 млн звонков (Александрова, 2023).

Проблема телефонных мошенников исследуется на уровне высших решений. Задачами кибербезопасности озадачены не только частные предприятия, но и государственные учреждения. Так, банки и компании в сфере кибербезопасности формируют собственные базы злоумышленников, расследуют инциденты и при помощи технологий создают библиотеки, в которых хранятся голосовые записи. Они помогают определять мошенников, если системы считывают соответствие голосов. В 2024 году Банк России инициировал блокировку почти 172 тыс. телефонных номеров злоумышленников, а также чуть больше 46 тыс. мошеннических сайтов и страниц в социальных сетях (Банки в 2024 году предотвратили вдвое больше мошеннических операций, 2024).

Так, Т-банк разработал сервис «Фрод-рулетка». С помощью него в режиме реального времени можно перехватывать звонки мошенников и разговаривать с ними анонимно. Буквально недавно в «Т-Дворе» в рамках ПМЭФ пранкеры Вован и Лексус с помощью сервиса выявили новую схему мошенничества. Сами создатели называют «рулетку» «сложным экспериментальным проектом, который уже на стадии раннего тестирования показывает феноменальные результаты».

Технологические инновации в борьбе с киберугрозами включают искусственный интеллект как основное средство для обнаружения аномалий. Современные системы на базе машинного обучения анализируют до 2,5 млн событий в секунду, выявляя 93% атак на этапе подготовки. Нейросетевые модели, используемые в Альфа-Банке и Сбербанке, демонстрируют точность 98,7% при классификации фишинговых попыток, обучаясь на датасетах из 500+ млн помеченных транзакций.

В 2024 году ВТБ внедрил квантово-устойчивые алгоритмы шифрования, совместимые с перспективными нейросетевыми системами обнаружения вторжений. Это позволило сократить время реакции на инциденты с 14 минут до 37 секунд (ВТБ предложит клиентам решения по кибербезопасности и облачным сервисам, 2024).

Таким образом, новейшие методы в сфере обеспечения финансовой безопасности российских банков разрабатываются с учетом современных технологических достижений и учитывают актуальные риски, такие как, телефонное мошенничество и повсеместное распространение искусственного интеллекта. Критически важным становится развитие компетенций в области квантовой криптографии и подготовка кадров для работы с гибридными системами ИИ.

Источники и литература

1) Александрова М.Ф. Замглавы Сбера: кибермошенники смещают фокус на менее защищенные организации / ТАСС // Москва, 2023. – URL: https://tass.ru/interviews/18696839 (дата обращения: 23.02.2025)

2) Банки в 2024 году предотвратили вдвое больше мошеннических операций. URL: https://cbr.ru/press/event/?id=23382 (дата обращения: 23.02.2025)

3) Васильева Ю.А. Методы оценки финансовой безопасности коммерческого банка // Форум молодых ученых. №1(77). 2023. С.66-70.

4) ВТБ предложит клиентам решения по кибербезопасности и облачным сервисам. URL: https://www.cnews.ru/news/top/2024-07-29_vtb_predlozhit_klientam_resheniya?erid=LjN8JzzSJ&ysclid=m7h7rfdsjo541588353 (дата обращения: 23.02.2025)

5) Лавров: потери мировой экономики от кибератак могут составить $8 трлн в 2022 году / Тасс // - Москва, 2020. – URL: https://tass.ru/ekonomika/9567725 (дата обращения: 23.02.2025)