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

Разработка методик для расследования финансовых преступлений, совершенных с использованием мобильных платежных приложений: анализ уязвимостей популярных платежных сервисов и разработка рекомендаций по их устранению.

Научный руководитель – Анищенко Александр Владимирович

Харазия София Саидовна

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия

E-mail: harazzzia@mail.ru

В последние годы наблюдается стремительное распространение мобильных платежных приложений, что обусловлено развитием мобильных технологий, ростом проникновения смартфонов и потребительским спросом на удобство и оперативность финансовых операций. Согласно отчету Statista [n7, Statista, 2021], объем мирового рынка мобильных платежей, по прогнозам, превысит 12 триллионов долларов к 2025 году, что отражает совокупный годовой темп роста более чем на 30 % с 2019 года.

В то же время эта эволюция сопровождается всплеском финансовых преступлений, использующих те самые технологии, которые призваны обеспечить простоту использования и доступность. Такие преступления не только подрывают безопасность финансовых операций, но и подрывают доверие к цифровым платежным системам, что требует комплексного подхода к их расследованию и предотвращению.

Анализ уязвимостей в мобильных платежных направлен на выявление технических, процедурных и человеко-ориентированных слабых мест, которыми пользуются киберпреступники.

Технические уязвимости: Значительная часть выявленных уязвимостей связана с техническими проблемами в инфраструктуре мобильных платежей. К ним относятся недостатки в механизмах шифрования, которые не обеспечивают должной защиты данных при передаче и хранении, делая конфиденциальную информацию уязвимой для перехвата и неправомерного использования.

Изучение технических и процедурных слабых мест в мобильных платежных приложениях позволяет получить критическое представление о том, как с помощью этих платформ совершаются финансовые преступления. Кроме того, неадекватные процедуры аутентификации, такие как использование однофакторной аутентификации или слабая парольная политика, способствуют несанкционированному доступу к учетным записям пользователей.

Уязвимости, связанные с процедурами и политикой: Процедурные уязвимости выявлены в операционных политиках и практике предоставления услуг мобильных платежей. К ним относятся отсутствие строгих процессов проверки новых пользователей, недостаточный мониторинг транзакций на предмет выявления аномальных закономерностей, указывающих на мошенничество, и несвоевременное внедрение исправлений и обновлений системы безопасности. Отсутствие надежных протоколов реагирования на инциденты еще больше усугубляет риск, препятствуя принятию своевременных мер в случае нарушения безопасности.

Уязвимости, связанные с пользователями: Человеческий фактор играет решающую роль в безопасности мобильных платежных систем. Уязвимости, связанные с пользователями, возникают из-за недостаточной осведомленности о методах безопасного проведения транзакций, таких как передача конфиденциальной информации по незащищенным сетям или фишинговые аферы. Отмечается тенденция пользователей обходить функции безопасности ради удобства, например, отключать многофакторную аутентификацию или использовать легко угадываемые пароли.

Устранив эти уязвимости, правоохранительные органы смогут значительно повысить устойчивость мобильных платежных систем к действиям киберпреступников, тем самым защитив данные пользователей и финансовые активы. Разработка методов расследования для борьбы с финансовыми преступлениями в мобильных платежных системах - важнейший компонент укрепления цифровой финансовой безопасности. В настоящее время используются следующие методы борьбы.

Инновационные методы обнаружения. Важнейшим аспектом разработанных методов расследования является применение инновационных технологий обнаружения.

Используя алгоритмы искусственного интеллекта и машинного обучения, эти методы способны анализировать обширные массивы данных для выявления закономерностей, указывающих на мошеннические действия. Обучая модели на исторических данных о транзакциях, включая известные случаи мошенничества, эти алгоритмы могут предсказывать и отмечать потенциальные мошеннические операции в режиме реального времени.

Цифровая криминалистика и прослеживаемость. Еще одним важным событием стало расширение возможностей цифровой криминалистики. Методы расследования теперь включают в себя передовые технологии отслеживания, которые позволяют отслеживать незаконные транзакции в сложных сетях цифровых финансов. Такие возможности отслеживания играют важную роль в подготовке доказательств для судебного преследования и возвращении похищенных активов.

Анализ поведения пользователей: Включение анализа поведения пользователей в методы расследования доказало свою эффективность в обнаружении аномалий, которые могут свидетельствовать о мошеннических действиях. Отслеживая взаимодействие пользователей с мобильными платежными приложениями, следователи могут выявить отклонения от обычных моделей поведения.

Разработка этих методов расследования знаменует собой значительный шаг на пути к снижению рисков, связанных с финансовыми преступлениями в системах мобильных платежей. Благодаря постоянным инновациям и сотрудничеству сообщество цифровых финансов может повысить свою устойчивость к киберпреступной деятельности, обеспечивая безопасность и надежность мобильных платежных платформ.

Источники и литература

1) Головин А. Ю. Проблемы и пути совершенствования методик расследования отдельных видов преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2014. № 3-2. С. 3–10

2) Куприянов Е.И Крашенинников С.В. Особенности производства отдельных следственных действий при расследовании преступлений, связанных с хищением денежных средств со счетов банковских карт посредством использования электронных платежных систем // Российский следователь. 2018. №6. С. 11-14.

3) Маилян, А.В. Совершенствование методики расследования хищения с использованием электронных средств платежа : автореферат дис. ... кандидата юридических наук / Маилян Ани Варужановна. Ростов-на-Дону, 2021. - 25 с.

4) Маилян А. В. Криминалистические аспекты изучения хищений, совершенных с использованием электронных средств платежа // Вестник УЮИ. 2020. №3 (89). С. 110-115.

5) Олиндер Н. В. Криминалистическая характеристика электронных платежных средств и систем // Lex Russica. 2015. № 10. С. 128–138.

6) Сидоренко Э.Л. Риски цифровизации и новые направления финансового контроля // Государственная служба. 2019. №1 (117). С.81-85.

7) Агрегатор статистической информации в отношении потребительских и рыночных данных «Statista»: офиц. сайт. URL: https://www.statista.com/statistics/871513/worldwide-data-created (дата обращения: 14.02.2024).