ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Кафедра информационной безопасности

Безопасность систем быстрых платежей: угрозы и меры защиты

Подготовил: студент группы УИБ25-2м, факультета информационных технологий и анализа больших данных, направление подготовки 10.04.01 Информационная безопасность (Управление информационной безопасностью в кредитно-финансовой сфере)
Матевосян Гурген Арменович

Москва - 2026

АКТУАЛЬНОСТЬ И ВВЕДЕНИЕ В ПРОБЛЕМУ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- СБП – критически важная инфраструктура с режимом работы 24/7/365.
- Рост объема транзакций = рост интереса злоумышленников.
- Уникальные риски: высокая скорость, необратимость платежа, массовость пользователей.
- Цель исследования: систематизировать угрозы безопасности в СБП и проанализировать комплекс мер защиты на различных уровнях.

АРХИТЕКТУРА СБП И ТОЧКИ ПРИЛОЖЕНИЯ УГРОЗ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Участники: Клиент (отправитель/получатель), Банк-отправитель, Банк-получатель, Оператор СБП (Банк России), Сервисы токенизации.

Ключевые точки риска:

- Канал связи «Клиент – Банк» (мобильное приложение, соц. инженерия).
- Фронтенд-системы банка (API, шлюзы).
- Операторский комплекс СБП (межбанковский обмен).
- Системы токенизации и биометрической аутентификации.

СБП

КЛАССИФИКАЦИЯ КЛЮЧЕВЫХ УГРОЗ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Вектор атаки	Цель / Механизм	Последствия
Социальная инженерия	Фишинг, вишинг, смишинг под видом службы безопасности банка или знакомого	Добровольный перевод средств клиентом
Клиентские устройства	Вредоносное ПО (трояны, кейлоггеры), взлом ОС, перехват SMS/уведомлений	Кража учетных данных, подтверждений
Атаки на банковские системы	Подбор/взлом API банка, DDoS на интерфейсы СБП, инъекции в системы процессинга	Массовые несанкционированные транзакции
Мошенничество с возвратами	Схемы «продажа товара – получение оплаты по СБП – оспаривание перевода»	Убытки для продавца, репутационные риски
Внутренние нарушители	Действия сотрудников банка или оператора, имеющих доступ к системам	Крупные утечки данных или хищения

АТАКИ НА API БАНКОВ-УЧАСТНИКОВ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Угроза: автоматизированные атаки на интерфейсы интеграции банка с СБП.

Механизмы:

- BIN-атаки: подбор номеров карт по известному банковскому идентификатору.
- Брутфорс авторизации: подбор одноразовых паролей (если слабая логика).
- Эксплуатация уязвимостей API (инъекции, неправильная настройка прав).
- Последствия: массовый, скрытый до момента слива денег, слив средств со счетов.

КОМПЛЕКС МЕР ЗАЩИТЫ НА СТОРОНЕ БАНКА-УЧАСТНИКА

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Усиленная аутентификация: многофакторная аутентификация (MFA) с привязкой к устройству, биометрия, анализ поведения.
- Защита API: использование стандартов (OAuth 2.0, OpenID Connect), WAF, ограничение скорости запросов (rate limiting), валидация входящих данных.
- Фрод-мониторинг в реальном времени: AI/ML-системы, анализирующие поведенческие паттерны, геолокацию, устройство, сумму, получателя.
- Сегментация и мониторинг: выделение сегмента сети для платежных систем, постоянный мониторинг SIEM/SOC.
- Регулярный аудит и тестирование: Пентесты, анализ уязвимостей, оценка соответствия СТО БР ИББС и PCI DSS.

МЕРЫ ЗАЩИТЫ НА УРОВНЕ ОПЕРАТОРА СБП

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Единая биометрическая система (ЕБС): дистанционная идентификация для минимизации рисков при первом переводе незнакомому лицу.
- Сервис токенизации: замена реквизитов карты/счета на уникальный токен. Даже при утечке данные бесполезны.
- Централизованный мониторинг и ФинЦЕРТ: анализ сетевой активности всех участников, оперативное оповещение об угрозах, координация при инцидентах.
- Регуляторное давление: установление стандартов безопасности (СТО БР ИББС), требований к фрод-мониторингу банков.

РОЛЬ КЛИЕНТА И ПРОБЛЕМЫ ИНФОРМИРОВАНИЯ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Проблема: Клиент — самое слабое звено, но и ключевой участник защиты.

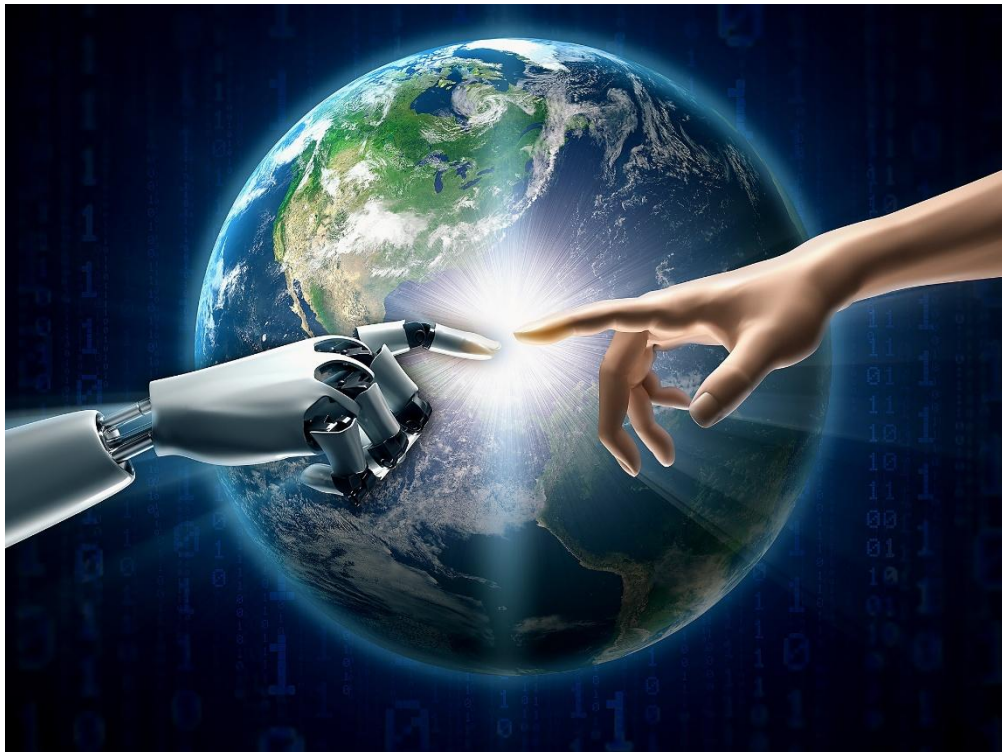
Что может/должен делать клиент:

- Никогда и никому не сообщать коды из SMS/push.
- Включать дополнительные проверки для переводов новым получателям.
- Использовать официальные приложения и регулярно их обновлять.
- Проверять номер получателя перед переводом.
- Задача банков и государства: Постоянные, навязчивые, понятные кампании по информированию.

ВЫЗОВЫ БУДУЩЕГО И ТЕНДЕНЦИИ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

- Борьба с социальной инженерией: внедрение proactive antifraud (системы, которые звонят клиенту при подозрительном действии).
- Децентрализованная идентификация: использование технологий Self-Sovereign Identity (SSI) на блокчейне.
- Постквантовая криптография: подготовка к угрозе взлома текущих алгоритмов шифрования.
- Ответственность экосистемы: распределение ущерба между банком, оператором связи, платформами-посредниками.



ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Спасибо за внимание!