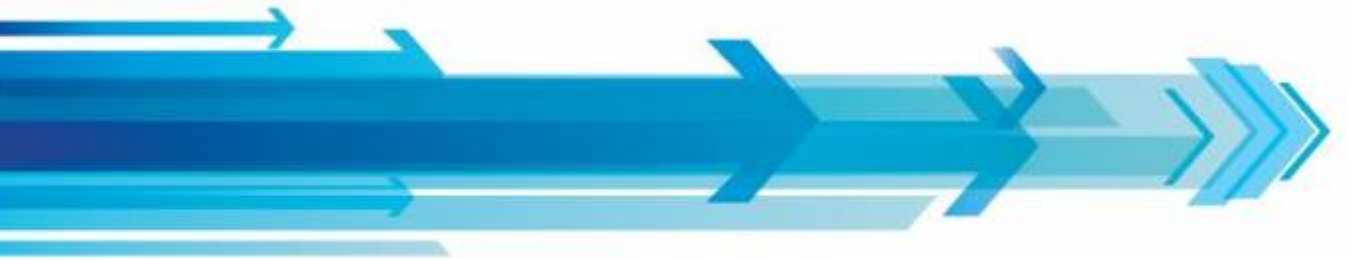
Центральный научно-исследовательский институт связи

О мерах по противодействию незаконным операциям с использованием модуля идентификации абонента при предоставлении услуг подвижной радиотелефонной связи



ФГУП ЦНИИС

Предпосылки мошенничества в сфере дистанционных платежей

Широкое распространение коммуникационных устройств среди населения, не подготовленного к противодействию мошенничеству

Использование технических средств для осуществления платежных операций в автоматическом режиме без личного присутствия владельца средств для осуществления платежа или передачи денег другому лицу

Движение денежных средств на основе единых принципов и правил коммуникации и платежей

Недочеты в законодательстве о платежах и услугах связи, Недостаточность мероприятий противодействия мошенникам

Отсутствие единой федеральной системы мониторинга мошеннических транзакций и противодействия хищениям электронных денег

Центральный научно-исследовательский институт связи

Характеристика мошеннических групп

Несколько участников группы имеют высшее образование и обладают навыками в области ИТ, а также в области психологии, НЛП и манипулирования.

Для хищения данных используются компьютеры, мобильные телефоны, современные средства коммуникации.

Организация строится по распределённому принципу, в связи с чем практически невозможно вычислить всех участников группы

Задания передаются через анонимные сетевые сервисы или по СМС, деньги переводятся на карты преступников через цепочку посредников

Как правило, преступление совершается в несколько этапов, реализация которых зачастую осуществляется участниками группы в различных странах

Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов.

Центральный научно-исследовательский институт связи

SMS-фишинг: схема мошенничества

Мошенники используют широковещательные рассылки, зачастую от имени Банка России, SMS-сообщений следующего содержания:

Ваша карта заблокирована, информация по телефону (903) 11111111

По Вашей карте запланирован платёж на сумму 33500 рублей. Для отмены позвоните по телефону (903) 11111111

Вам поступил платёж на сумму 5768 фунтов стерлингов. Подтвердите получение, иначе платеж будет возвращён отправителю. Телефон для справок (903) 11111111

Поздравляем! Вы выиграли компьютер! Информация (800) 11111111

Цель сообщения - инициировать звонок держателя карты мошенникам. Во время звонка клиента убеждают подойти к банкомату и выполнить ряд процедур либо выясняют конфиденциальную информацию о карте, системе ДБО, кодовые слова …..

В результате клиент сам переводит денежные средства на карту или счет мобильного телефона мошенников, либо сообщает все данные карты, SMS пароли, кодовые слова затем мошенники переводят и обналичивают полученные средства.

Центральный научно-исследовательский институт связи

Замена SIM карты: схема мошенничества

Мошенники используют недостатки в системе безопасности мобильных операторов и служб ДБО банков:

Методами фишинга (социальной инженерии) во время разговора с гражданином получают персональные данные (серия, номер паспорта, номер мобильного телефона), или через троянские программы проникают на домашний компьютер и находят всю информацию там, включая логин и пароль для входа в интернет банк

Изготавливают поддельные документы (паспорт, водительское удостоверение, нотариальная доверенность)

Получают в отделении оператора мобильной связи дубликат SIM карты, вставляют (обычно ночью) карту в свой телефон, после чего телефон законного владельца перестает работать, а мошенники получают все SMS направленные владельцу, в том числе банковские

Цель – Получить доступ к данным мобильного телефона либо к интернет банку и украсть деньги со счета в банке, пластиковой карты, счета мобильного телефона.

Центральный научно-исследовательский институт связи

Кража средств через Интернет-Банк (в т.ч. при наличии двухфакторной аутентификации)

Схема мошенничества более подробно:

1. Внедрение на компьютер жертвы вредоносной троянской программы либо манипулирование поведением жертвы по телефону с использованием методов НЛП и социальной инженерии.
2. Получение информации о персональных данных, номерах счетов и карт.
3. Получение дубликата SIM карты в офисе оператора по поддельному паспорту, водительскому удостоверению, нотариальной доверенности.
4. Мониторинг финансовых потоков жертвы, выбор момента совершения преступления
5. Использование дубликата SIM карты в телефоне мошенников, перехват сообщений.
6. Хищение средств и перевод их на банковские счета, карты, счета мобильных телефонов или электронные кошельки, контролируемые мошенниками
7. Снятие наличных денежных средств либо покупка товаров и услуг для последующей перепродажи.

Этапы преступления

Массовые рассылки SMS сообщений, внедрение троянских программ, звонки на мобильные телефоны с целью получения от гражданина персональных данных и конфиденциальной информации.

Получение доступа к телефону или компьютеру гражданина.

Перевод средств на счета, карты или электронные кошельки, контролируемые мошенниками

Создав адекватную систему предотвращения мошенничества, заблокировав возможности по рассылке фишинговых SMS сообщений и несанкционированной замене SIM карт, усилив контроль за продажей контрактов мобильных операторов, можно существенно затруднить для преступников процесс использования похищенных средств, осуществить оперативную блокировку и возврат похищенных сумм.

Центральный научно-исследовательский институт связи

Возможные мероприятия по предотвращению и пресечению мошенничества

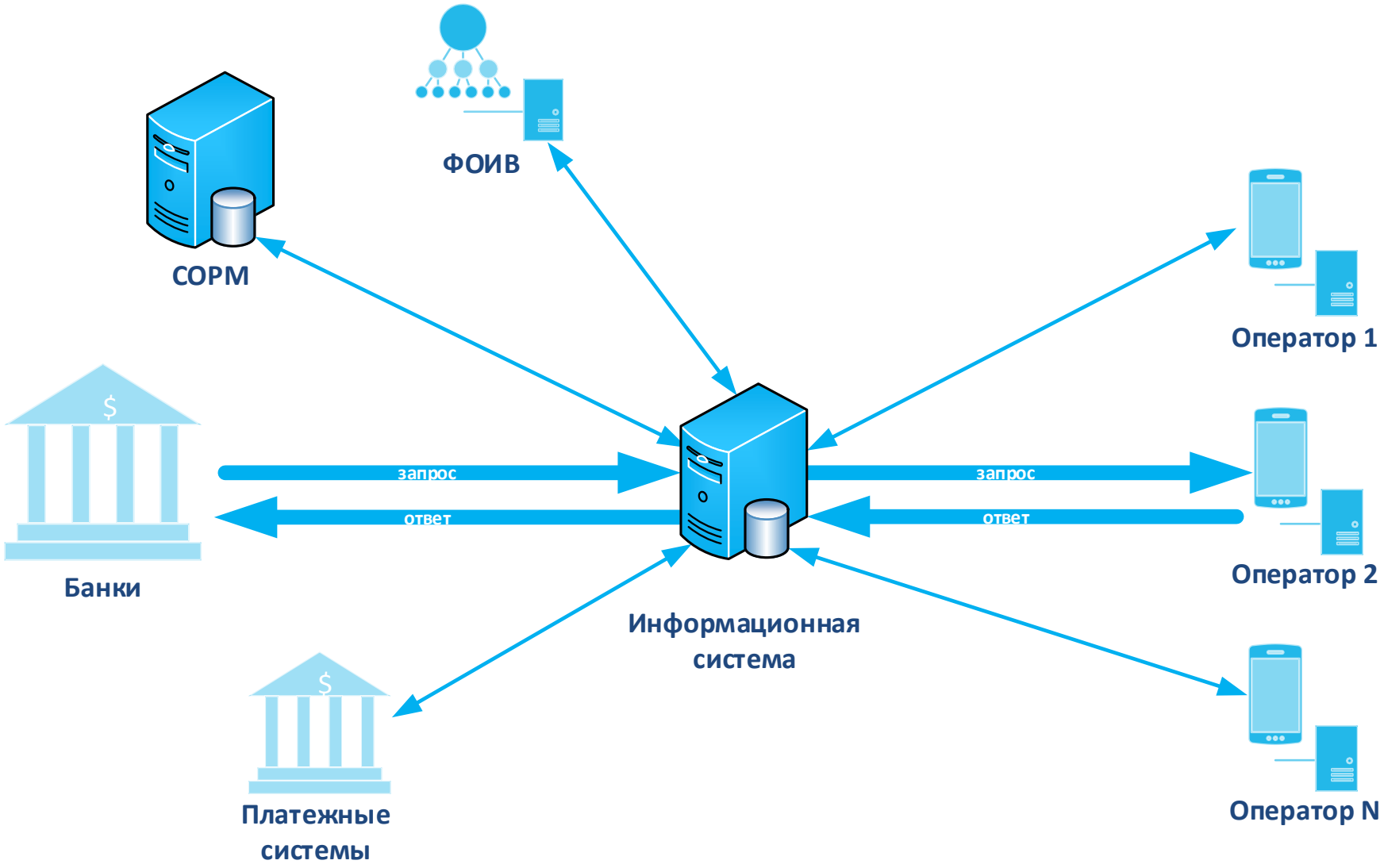
- ☑ Совершенствовать законодательную базу в части мобильной связи и электронного денежного оборота, в том числе усилить ответственность за преступления в области высоких технологий.
- ☑ Сформировать единые правила для всех операторов мобильной связи с установлением ответственности за бездействие при мошенничестве с использованием оборудования или программного обеспечения оператора.
- ☑ Обеспечить эффективный государственный надзор за надлежащим проведением идентификации клиентов в целях полного соблюдения законодательства о ПОД/ФТ (противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансировании терроризма).
- ☑ Усилить работу по формированию ответственного экономического поведения и повышению финансовой грамотности населения, особенно в части безопасного использования электронных средств платежа.

Единая информационная система

Что даст её создание?

- ✓ Единый сервис для получения информации от операторов связи
- ✓ Дополнительная верификация пользователей
- ✓ Актуализация абонентских баз коллекторских служб
- ✓ Повышение уровня защищенности граждан – абонентов подвижной радиотелефонной связи
- ✓ Повышение уровня безопасности переводов денежных средств с использованием мобильного телефона
- ✓ Надлежащее исполнение кредитными и иными финансовыми организациями нормативных требований

Необходимая ИКТ-инфраструктура



Состав предоставляемой информации

1) Сведения о подтверждении соответствия абонентского номера сети подвижной радиотелефонной связи и фамилии, имени, отчества (при наличии) абонента, предоставленных физическим лицом – абонентом в кредитную организацию (иную организацию, определенную Правительством Российской Федерации).

2) При условии указания в запросе сведений о фамилии, имени, отчестве (при наличии) абонента, номера документа, удостоверяющего личность абонента, и абонентского номера сети подвижной радиотелефонной связи, соответствующих сведениям об абоненте, имеющимся у оператора подвижной радиотелефонной связи, следующие сведения:

- дата заключения действующего договора об оказании услуг подвижной радиотелефонной связи;
- дата выдачи абоненту подвижной радиотелефонной связи модуля идентификации абонента;
- дата последней замены (выдачи дубликата) модуля идентификации абонента абоненту подвижной радиотелефонной связи.

СПАСИБО!

Адрес: 111141, г. Москва, 1-й проезд Перова поля, д. 8
Тел.: +7 (495) 304-5797
Тел./факс: +7 (495) 674-0067
E-mail: info@zniis.ru
www.zniis.ru