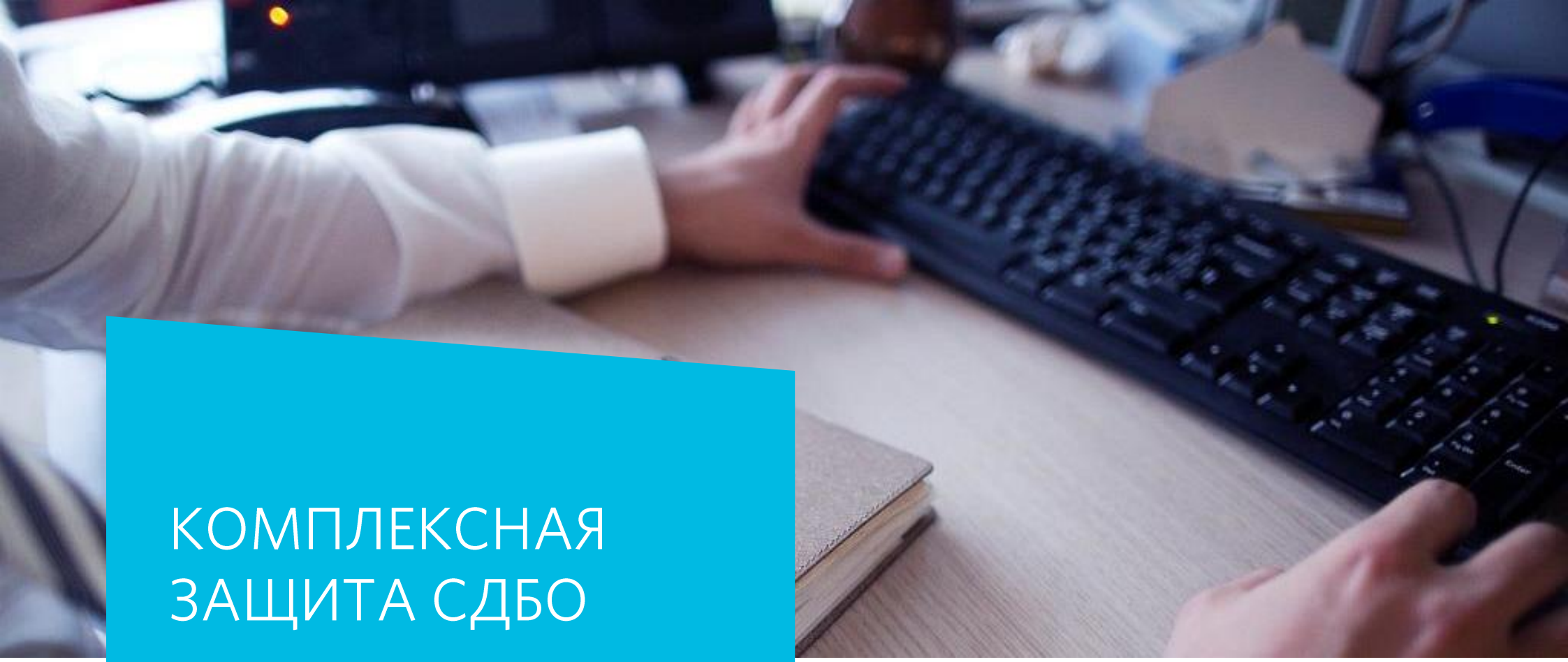


# КОМПЛЕКСНАЯ ЗАЩИТА СДБО

В жизни всегда
есть место открытию

openbank.ru

открытие | БАНК

# ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

ДБО — общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (т.е. без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей.

---

## Виды ДБО:

- **«Толстый клиент»** — на рабочей станции пользователя устанавливается отдельная программа – клиент. Преимущество в отсутствии необходимости постоянного подключения к банковской части ДБО
- **«Тонкий клиент»** — для доступа к ДБО используется Интернет браузер. Преимущество – мобильность и невысокая стоимость эксплуатации
- **Мобильный банкинг** — зачастую программа – клиент, устанавливаемая на Personal Digital Assistant (PDA – смартфон, планшет) устройство клиента. Преимущество – удобство использования
- **Телефонный банкинг, SMS — банкинг**
- **Обслуживание с использованием банкоматов и платежных терминалов**

# ПРИМЕР АБСОЛЮТНО
# БЕЗОПАСНОГО ПЛАТЕЖА

Абсолютно безопасных платежей не существует

# ПОЧЕМУ ХИЩЕНИЯ ВОЗМОЖНЫ?

- Незащищенность компьютеров от современных вирусов (антивирусное программное обеспечение не эффективно)
- Массовые заражения крупнейших легальных сайтов вирусами
- Возможность удаленно управлять зараженным компьютером через сеть интернет
- Низкая компьютерная грамотность

## ПОСЕЩЕНИЕ ЗАРАЖЕННЫХ САЙТОВ

(бухгалтерские ресурсы, сайты банков, бизнес новости и т.д.)

Заражение компьютера

- Удаленное управление
- Проброс USB портов
- Подмена платежа

Хищение средств с расчетного счета

# КАК «ТАМ» ОРГАНИЗОВАНО

- Мошеннические действия со стороны организованных групп с распределением по регионам и ролям — 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

- Несколько участников группы имеют высшее образование и обладают навыками в области ИТ, психологии, знают приемы НЛП

- Как правило, преступление совершается в несколько этапов, реализация которых может осуществляться участниками группы в различных странах

# КАК «ТАМ» ОРГАНИЗОВАНО

- Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов
- Для хищения используются компьютеры, мобильные телефоны, современные средства коммуникации
- Заблаговременно подготовленное обналичивание средств:

Банковские карты

Платежные системы

Электронные кошельки

Мобильные телефоны

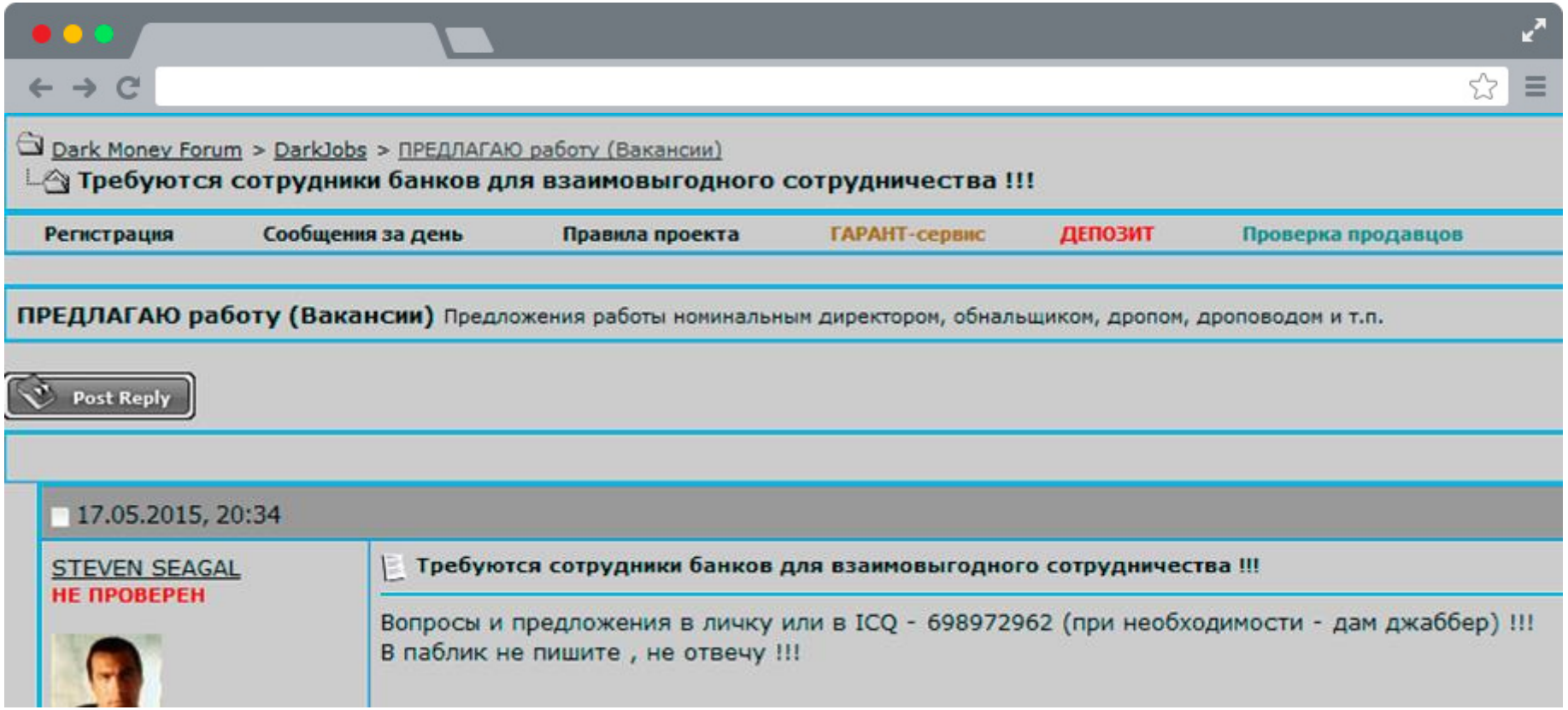
# КАК «ТАМ» ОРГАНИЗОВАНО


## Еженедельный доход

Киберпреступников от троянской программы Carberp, поражающей систему дистанционного банковского обслуживания (ДБО), в России достигал **$10 млн**, отмечают аналитики компании, разработчика известной антивирусной программы NOD32 (источник)

# АКТУАЛЬНАЯ МОДЕЛЬ
# ЗЛОУМЫШЛЕННИКА

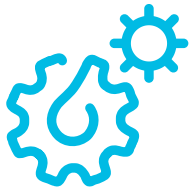
- Внешний высококвалифицированный злоумышленник (традиционно)
- Внешний злоумышленник средней или высокой квалификации с пособником в Банке (свежий тренд)



# МНОГООБРАЗИЕ УГРОЗ
# И УЯЗВИМОСТЕЙ

Организационные

Направленные
на клиента



Направленные
на банк

# МНОГООБРАЗИЕ УГРОЗ
# И УЯЗВИМОСТЕЙ

## Организационные

- Подключение / переподключение ДБО вместо клиента
- Несоответствие условий ДБО
- Юридические уязвимости в условиях ДБО
- Отсутствие полного комплекта документов (утрата / кража)

## Направленные на клиента

## Направленные на банк

# МНОГООБРАЗИЕ УГРОЗ И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

- Социальная инженерия
- Фишинг
- Удаленное управление устройством пользователя
- Модификация платежного поручения перед его подтверждением на стороне клиента вредоносным ПО
- Кража паролей и ключей (в том числе одновременно с кражей устройства)

# МНОГООБРАЗИЕ УГРОЗ
# И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

- Уязвимости прикладного уровня
- Внесение нелегитимных изменений в настройки серверной части
- Удаленное управление инфраструктурой банка
- Недостаточная связь подписи с параметрами платежа
- Отсутствие механизмов выявления мошеннических транзакций
- Мошеннические действия персонала

# МНОГООБРАЗИЕ УГРОЗ И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

| Вид уязвимости | Описание | Уровень риска | Описание риска |
|---|---|---|---|
| Подключение / переподключение ДБО вместо клиента | Уязвимости в процессах подключения/переподключения клиенту ДБО.<br>Может реализовываться как с участием сотрудников Банка, так и по причине некорректно выстроенных процессов | | Остается на высоком уровне в связи с недостаточным фокусом на безопасность и прозрачность процессов, ограничение прав сотрудников, а так же контроль их действий |
| Несоответствие условий ДБО<br><br>Юридические уязвимости в условиях ДБО | Некорректно составленные договорные отношения с клиентом, в т.ч. не полностью предусматривающие соответствие законодательству РФ. | | Могут быть единичные случаи реализации риска. При этом реальной практики мало. |
| Отсутствие полного комплекта документов (утрата / кража) | Отсутствие у банка документов/ неполный комплект документов, подтверждающих намерения клиента использовать систему ДБО | | Риск может реализоваться при сговоре с сотрудниками банка. Реальной практики подобных судебных разбирательств мало. |

# МНОГООБРАЗИЕ УГРОЗ И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

| Вид уязвимости | Описание | Уровень риска | Описание риска |
|---|---|---|---|
| Социальная инженерия | Клиент сам передает злоумышленнику все параметры для аутентификации. Это ключевая уязвимость использования только подхода «я знаю» | | Снижается в связи с ростом компьютерной грамотности клиентов Банка |
| Фишинг | Рассылка смс, в. т.ч. с буквенного адреса с целью получения кодов ОТП, паролей, данных карт, персональной информации | | Снижается в связи с ростом компьютерной грамотности клиентов Банка |
| Удаленное управление устройством Клиента<br><br>Модификация платежного поручения<br><br>Кража паролей и ключей | Заражение или получение доступа к устройству клиента. (Троян, включая перехват управления). Далее кража закрытого ключа, удаленное управление, подмена платежа, искажение информации в браузере или подмена документа при передаче его на подпись в смарт-карту. Это ключевая проблема подхода «я имею» и «я есть» в случае совмещения устройств для платежей и аутентификации. | | Активность мошенников растет, постоянно появляются новые приемы и способы взлома, существует развитый рынок вредоносного ПО |

# МНОГООБРАЗИЕ УГРОЗ И УЯЗВИМОСТЕЙ

Организационные

Направленные на клиента

Направленные на банк

| Вид уязвимости | Описание | Уровень риска | Описание риска |
|---|---|---|---|
| Уязвимости прикладного уровня | Уязвимости в прикладной части ДБО, позволяющие манипулировать счетами/параметрами платежей | | ДБО – система, подверженная постоянной модификации, что влечет за собой появление новых уязвимостей |
| Внесение изменений в серверную часть | Некотролируемые/нелигитимные изменения могут повлечь критичные уязвимости инфраструктуры | | Появление критичных уязвимостей в инфраструктуре ДБО могут привести к компрометации ДБО и/или клиентов Банка |
| Удаленное управление инфраструктурой | Уязвимости архитектуры, инфраструктуры и/или приложений, которые могут привести к получению злоумышленником доступа для управления инфраструктурой Банка | | Активность мошенников растет, постоянно появляются новые приемы и способы взлома, существует развитый рынок вредоносного ПО |
| Недостаточная связь подписи с платежом | Подпись для подтверждения операции не связана с параметрами платежа | | Пример – случайно сгенерированный ОТП. Реальной судебной практики мало. |
| Отсутствие antifraud | Отсутствие механизмов выявления мошеннических транзакций | | Отсутствие механизмов дает возможность массового хищения средств при обнаружении уязвимостей аутентификации |
| Мошеннические действия персонала | Изменение/компрометация данных клиента и похищение второго фактора аутентификации (ключевая проблема подхода «я имею» в случае не полного контроля второго фактора клиентом) | | Сумма ущерба может быть значительна при отсутствии аудита доступа к клиентским данным, сговоре нескольких сотрудников из разных звеньев бизнес процесса |

# ПРИМЕР СХЕМЫ МОШЕННИЧЕСТВА

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

# ПРИМЕР СХЕМЫ SMS, E-MAIL-ФИШИНГА

- Мошенники используют широковещательные рассылки, зачастую от имени Банка России, E-mail, SMS-сообщений **следующего содержания**:
  - Ваша карта заблокирована, информация по телефону (903) 111-11-11
  - По Вашей карте запланирован платёж на сумму 33500 рублей. Для отмены позвоните по телефону (903) 111-11-11
  - Вам поступил платёж на сумму 5768 фунтов стерлингов. Подтвердите получение, иначе платеж будет возвращён отправителю. Телефон для справок (903) 111-11-11
  - Поздравляем! Вы выиграли компьютер! Информация (800) 111-11-11

- **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.

# ОГРАНИЧЕНИЯ ДЛЯ ЗАЩИТЫ

## Клиентоориентированный подход

- подключение для клиента должно быть простым, понятным, требующим минимум визитов в банк;
- клиента не должен беспокоить фрод-мониторинг, общение должно происходить только в действительно подозрительных случаях.

## Низкий фокус и объем затрат на ИБ

- затраты должны быть ниже оцененных рисков краж у клиентов, рассчитанных на основе статистики и подходов к обработки хищений банком (возвращаются д/с или нет);
- максимум превентивных мер, низкий OPEX.

## Критерии успеха защиты

«Клиенту еще удобно – мошеннику уже не выгодно»

- Безопасность – это совокупность мер, предполагающих правильное построение процессов безопасности с учетом:
  - технологических решений
  - организационных мер
- Оценка рисков, финансовых последствий возможных угроз и затрат на борьбу с мошенниками.

# СПОСОБЫ ЗАЩИТЫ

## Защита серверной части

- Контроль целостности ДБО
- Регулярный анализ событий ИБ
- Управление уязвимостями
- Анализ исходного кода
- Контроль действий администраторов
- Ограничение доступа к ДБО
- Защита периметра

## Организационные меры

- Обеспечение юридической значимости действий клиента в ДБО
- Выстроенные процедуры реагирования на инциденты
- Управление изменениями
- Страхование рисков

## Надежная аутентификация

- Обязательный секрет, доступ к которому есть только у клиента
- Двухфакторная аутентификация с привязкой к параметрам транзакции
- Создание схемы, когда только клиент обладает всеми параметрами для подключения к интернет-банку

## Повышение осведомленности клиентов

- Доступные и заметные инструкции
- Донесение необходимости принятия мер по защите устройств клиента

## Защита от внутреннего злоумышленника

- Контроль действий персонала
- Ролевая модель

## Антифрод

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов

# СПОСОБЫ ЗАЩИТЫ

## Защита серверной части

- **Контроль целостности ДБО**
- **Регулярный анализ событий ИБ**
- Управление уязвимостями
- Анализ исходного кода
- Контроль действий администраторов
- Ограничение доступа к ДБО
- Защита периметра

## Контроль целостности ДБО

- Определение критичных параметров для контроля
- Внедрение механизмов контроля целостности
- Внедрение процесса управления изменениями

## Регулярный анализ событий информационной безопасности

- Определение критичных событий для сбора
- Определение правил корреляции событий
- Внедрение процесса реагирования на инциденты

# СПОСОБЫ ЗАЩИТЫ

## Защита серверной части

- Контроль целостности ДБО
- Регулярный анализ событий ИБ
- **Управление уязвимостями**
- **Анализ исходного кода**
- Контроль действий администраторов
- Ограничение доступа к ДБО
- Защита периметра

## Управление уязвимостями

- Регулярное внутреннее и внешнее сканирование на уязвимости
- Патч менеджмент
- Регулярные тестирования на проникновение, а так же после существенных изменений в ДБО

## Анализ исходного кода

- Регулярный анализ исходного кода на ошибки программирования
- Анализ исходного кода перед выводом в эксплуатацию
- Контроль версий

# СПОСОБЫ ЗАЩИТЫ

## Защита серверной части

- Контроль целостности ДБО
- Регулярный анализ событий ИБ
- Управление уязвимостями
- Анализ исходного кода
- **Контроль действий администраторов**
- **Ограничение доступа к ДБО**
- **Защита периметра**

## Контроль действий администраторов, ограничение доступа

- Регистрация и контроль действий администраторов
- Периодический пересмотр пользователей и их прав

## Защита периметра

- Анализ угроз
- Периодический пересмотр правил сетевого доступа
- Внедрение технических и организационных мер защиты периметра

# СПОСОБЫ ЗАЩИТЫ

## Надежная аутентифи

- **Обязательный секрет, доступ к которому есть только у клиента**
- Двухфакторная аутентификация с привязкой к параметрам транзакции
- Создание схемы, когда только клиент обладает всеми параметрами для подключения к интернет-банку

## Идентификация

- на основании представленной клиентом информации

## Аутентификация

- процедура, позволяющая установить подлинность лица, получающего доступ к автоматизированной системе, путем сопоставления  идентификатора и предъявленных подтверждающих факторов

## Авторизация

- процедура предоставления прав определённому объекту, субъекту или процессу на выполнение определенный деятельности (например, доступ к данным)

# СПОСОБЫ ЗАЩИТЫ

## Надежная аутентифи

- Обязательный секрет, доступ к которому есть только у клиента
- **Двухфакторная аутентификация с привязкой к параметрам транзакции**
- Создание схемы, когда только клиент обладает всеми параметрами для подключения к интернет-банку

## Многофакторная аутентификация

- Основной принцип заключается в использовании 2х или 3х независимых параметров:
  - Я знаю (например, пароль)
  - Я обладаю (чем то уникальным (мобильным устройством или криптографическим ключом)
  - Я есть (например, отпечаток пальца или сетчатка глаза)

## Двухфакторная аутентификация

может и должна осуществляться для любых критичных операций, позволяющих управлять счетом клиента:

- При подключении клиента (клиент вводит пароль и ему отправляется смс с кодом)
- Входе клиента в ДБО (клиент вводит пароль и OTP)
- Платеже клиента (клиент обладает токеном с ключом и знает пароль от токена)

# СПОСОБЫ ЗАЩИТЫ

## Надежная аутентифи

- Обязательный секрет, доступ к которому есть только у клиента
- Двухфакторная аутентификация с привязкой к параметрам транзакции
- **Создание схемы, когда только клиент обладает всеми параметрами для подключения к интернет-банку**

## Надежная схема

- Необходимо проанализировать все возможности получения клиентом параметров для доступа в ДБО
- Необходимо для каждой такой возможности оценить пути мошенничества и возможные риски

Примеры:

- При использовании sms-OTP регистрировать IMSI клиента и в случае его смены отправлять в отделение банка или банкомат для проведения повторной идентификации/аутентификации
- При переподключении ДБО или сбросе пароля для ДБО через колл центр запрашивать дополнительную аутентификацию клиента.

# ЭВОЛЮЦИЯ СРЕДСТВ АУТЕНТИФИКАЦИИ

| Уровень защиты | Уровень атаки | |
|---|---|---|
| ЭП с хранением ключей на незащищенном носителе | Хищение ключей с незащищенных носителей | Прошлое |
| ЭП с хранением ключей на защищенном носителе | Хищение ключей из оперативной памяти | |
| Персональное аппаратное СКЗИ (смарт карта, токен) | Несанкционированный доступ к возможностям токена | Настоящее |
| Сочетание аппаратного СКЗИ и одноразовых паролей OTP | Подмена документа при передаче его в токен | |
| Применение внешнего устройства с контролем платежа | | Будущее |

Злоумышленники атакуют наименее защищенные Банки (кого проще)
Не имеет смысла идти в «будущее» пока другие в «прошлом»

# ОБЗОР РЫНКА
# СРЕДСТВ АУТЕНТИФИКАЦИИ (часть 1)

| Вид аутентифкатора | Описание | Уровень риска | Описание |
|---|---|---|---|
| Token (smart-card) | Использование | Средний | Уязвимы к атакам «человек в браузере» |
| One Time Password (OTP) | SMS – OTP<br>e-mail OTP<br>push OTP<br>Программные токены (OTP)<br>Автономные генераторы OTP | Средний/высокий | Возможна одновременная компрометация устройства с OTP и компьютера. |
| Сертификат/ключ на устройстве | Аутентификация средствами ключа, который хранится на том же устройстве, с которого происходит платеж | Низкий | Уязвимы к похищению ключа, а так же атакам троянскими программами |
| Аутентификаторы на устройствах | Например, Google Authenticator. При использовании этой функции для входа в аккаунт необходимо вводить не только пароль, но и код, сгенерированный приложением | Средний | Возможна одновременная компрометация смартфона и компьютера. |
| Биометрика (палец, лицо или глаз) | Прохождение биометрической аутентификации на устройстве, с которого происходит платеж. | Средний/Высокий | Зависит от реализации. Главная проблема – троянская программа может подменить платеж после прохождения аутентификации. |
| Аутентификационные таблицы, скретч карты | Заранее выданные клиенту таблицы паролей, которые используются для аутентификации | Низкий | Уязвимы к фишингу, атакам «человек посередине» и «человек в браузере» |
| T-pin и звонок | Выдача клиенту специального телефонного пароля для аутентификации и использования сервисов колл центра | Низкий | |

# ОБЗОР РЫНКА
# СРЕДСТВ АУТЕНТИФИКАЦИИ (часть 2)

| Вид аутентифкатора | Описание | Уровень защиты | Риски использования |
|---|---|---|---|
| Поведенческий анализ | Аутентификация на основе анализа скорости ввода символов, перемещения мыши (клавиатурный почерк) | Высокий | Не известны троянские программы, способные перехватить и подделать поведение клиента |
| NFC на смартфонах | Банковское приложение, которое привязывается к номеру телефона. Приложение запароливается, с учетом особенности: после ввода пароля, вам нужно приложить телефон к NFC-карте, которую выдал банк для контрольного подписания данных. Телефон передает номер на карту через технологию NFC. Банковская карта самостоятельно каждый раз генерирует уникальный код, который совпадает с кодом в системе банкинга | Высокий | Не известны |
| Sim-меню | Аутентификация через меню своего телефона | Средний | Возможно одновременное заражение смартфона и компьютера |
| Аутентификационные браслеты | Браслеты, аутентифицирующие по параметрам человека, например - сердцебиению | Не известно | Недостаточно информации по статистике и реализации |
| Голосовая аутентификация | Анализ параметров голоса Клиента для аутентификации. Например, при совершении клиентом платежа Банк может перезвонить клиенту и аутентифицировать его по голосу. | Высокий | Присутствует дополнительный фактор аутентификации (телефонная линия) |
| QR-код нового поколения | QR-код здесь представляет собой цветную криптографическую матрицу, содержащую реквизиты платежного поручения. Есть программные и аппаратные решения | Высокий | Не известны |

# ОБЗОР РЫНКА
# СРЕДСТВ АУТЕНТИФИКАЦИИ (часть 3)

| Вид аутентифкатора | Описание | Уровень защиты | Риски использования |
|---|---|---|---|
| EMV CAP (Europay MasterCard Visa Chip Authentication Program ) | Аутентификация платежей средствами специального криптокалькулятора, в который вставляется карта для расчёта одноразового пароля, соответствующего транзакции | Высокий | Не известны |
| Криптокалькулятор | Аутентификация платежей средствами специального криптокалькулятора, в который вводятся параметры платежа для расчета одноразового пароля, соответствующего транзакции | Высокий | Не известны |
| Аутентификация на устройстве, не связанном с компьютером | Любое устройство, которое не связано с компьютером или связано только однонаправленно (на получение параметров платежа от компьютера). Как пример — устройства Safe touch | Высокий | Не известны |

# ВЫВОД ПО СРЕДСТВАМ АУТЕНТИФИКАЦИИ ДБО

- Наиболее защищенным способом аутентификации является **out of band устройство** — отдельное от компьютера устройство, которое не может быть заражено троянской программой, даже при подключении к компьютеру (не смартфон)

- Наиболее перспективным и развитым средством аутентификации являются подтверждение платежей при помощи out of band устройств (расчёт контрольного числа на таком устройстве на основе параметров платежа)

- Учитывается критерий качества — Клиенту еще удобно, а мошеннику уже не выгодно



# СПОСОБЫ ЗАЩИТЫ

## Организационные меры

- **Обеспечение юридической значимости действий клиента в ДБО**
- **Выстроенные процедуры реагирования на инциденты**
- Управление изменениями
- Страхование рисков

## Обеспечение юридической значимости действий клиента в ДБО

- Контроль изменений законодательства
- Контроль судебной практики
- Периодический пересмотр договорных отношений с клиентами

## Выстроенные процедуры реагирования на инциденты

- План реагирования на различные типы инцидентов ДБО
- Подготовленные процессы реагирования на известные инциденты
- Обученная группа реагирования

# СПОСОБЫ ЗАЩИТЫ

## Организационные меры

- Обеспечение юридической значимости действий клиента в ДБО
- Выстроенные процедуры реагирования на инциденты
- **Управление изменениями**
- **Страхование рисков**

## Управление изменениями

- Выстроенный процесс управления изменениями
- Тестирование исходного кода и поиск уязвимостей при существенных изменениях

## Страхование рисков

- Страхование рисков клиентов – как услуга для клиента
- Страхование рисков Банка
  - BBB – Bankers Blanked Bond – страхование от преступлений
  - ECC – Electronic & Computer Crime – от электронных и компьютерных преступлений

# СПОСОБЫ ЗАЩИТЫ

## Повышение осведомленности клиентов

- **Доступные и заметные инструкции**
- **Донесение необходимости принятия мер по защите устройств клиента**

## Доступные и заметные инструкции

- Простые и понятные инструкции
- Публикация security tips на странице входа в ДБО и сайте Банка
- Рассылки клиентам о новых способах мошенничества

## Донесение необходимости принятия мер по защите устройств клиента

- Инструкции с указанием конкретных шагов для защиты устройств
- Включение требований отдельным разделом в правила работы с ДБО
- Реагирование клиента на нестандартные ситуации (звонок/смс из банка, дополнительные окна с запросом данных на странице ДБО)

# СПОСОБЫ ЗАЩИТЫ

## Повышение осведомленности клиентов

- **Доступные и заметные инструкции**
- Донесение необходимости принятия мер по защите устройств клиента

## Инструкции для клиента

- Используйте сложные пароли
- Никому не передавайте данные для входа в систему, в т.ч. сотрудникам Банка
- При использовании одноразовых паролей по SMS, с особым вниманием отнеситесь к тому, что доступ 3х лиц к телефону невозможен
- Перед вводом кода подтверждения операции из SMS всегда проверяйте параметры операции, содержащиеся в сообщении
- Если это возможно, используйте выделенный компьютер для работы с ДБО (для юр лиц)
- Вход в систему с чужого компьютера (в интернет-кафе) не является безопасным
- Установите и настройте антивирусное программное обеспечение
- Регулярно устанавливайте обновления безопасности
- Подключите смс-информирование об операциях по счету
- При подозрении, что ваши данные для входа в систему стали известны третьим лицам, утере телефона устройства, которое вы используете для подтверждения операций в системе или обнаружении несанкционированных операций в системе, незамедлительно обратитесь в Банк
- Установите лимиты

# СПОСОБЫ ЗАЩИТЫ

## Защита от внутреннего злоумышленника

- **Контроль действий персонала**
- **Ролевая модель**

## Контроль действий персонала

- Определение критичных событий регистрации
- Сбор событий
- Контроль утечки данных

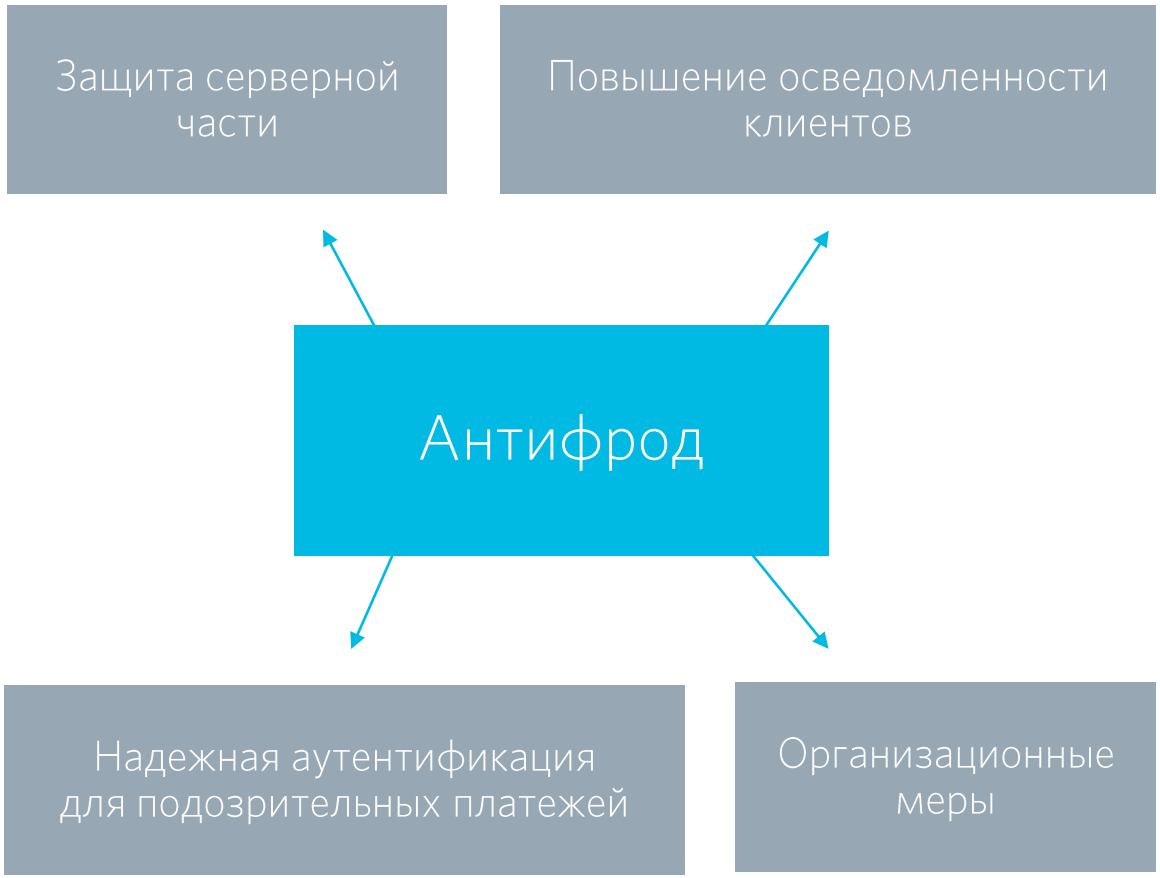
## Ролевая модель

- Регулярный пересмотр доступа сотрудников к компонентам ДБО
- Регулярный пересмотр ролевой модели с учетом принципов
  - Минимальной необходимости
  - Разделения полномочий при выполнении критичных операций

# СПОСОБЫ ЗАЩИТЫ

## Антифрод

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов




## Принципы работы:

- Блокировка платежей на этапах обработки в бэк-офисных системах
- Профили клиентов и их транзакций
- Возможность сравнения любых параметров платежей, клиентов, их входов в СДБО
- Не компонент СДБО
- Фиксация всех взаимодействий с клиентами

## Решаемые задачи:

- Интеллектуальная блокировка транзакций без необходимости постоянного отвлечения клиентов
- Противодействие внешним атакам на серверную часть
- Возможность донесения до клиентов как им защититься самостоятельно
- Реагирование на инциденты и дополнительные подтверждения авторства транзакций

# ВОПРОСЫ

Директор Департамента информационной безопасности

ГАДАРЬ
Дмитрий Александрович

Dmitry.Gadar@open.ru