|  |  |
| --- | --- |
| *voenmeh* | МИНОБРНАУКИ РОССИИ  федеральное государственное бюджетное образовательное учреждение  высшего профессионального образования  **«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»**  **(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова»)** |
| БГТУ.СМК-Ф-4.2-К5-01 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Факультет |  | И | |  |  | Информационные и управляющие системы |
|  |  | шифр | |  |  | наименование |
| Кафедра |  | И9 | |  |  | Систем управления и компьютерных технологий |
|  |  | шифр | |  |  | наименование |
|  |  |  |  | | | |

|  |
| --- |
| ОТЧЕТ |
| **ИССЛЕДОВАНИЕ проблем обеспечения информационной** |
| **безопасности в сфере банковской деятельности на примере УСЛУГ** |
| **дистанционного банковского обслуживания** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент группы | | | |  | | И9М31 |
| Загута Д.В. | | | | | | |
| Фамилия И.О. | | | | | | |
| **РУКОВОДИТЕЛЬ** | | | | | | |
| Романов Л.С. | |  |  | | | |
| Фамилия И.О. Подпись | | | | | | |
| Оценка |  | | | |  | |
| «\_\_\_\_\_» |  | | | | 2018 г. | |

САНКТ-ПЕТЕРБУРГ

2018 г.

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc2251442)

[1 ПРОБЛЕМА МОШЕННИЧЕСТВА В СИСТЕМАХ ДБО 3](#_Toc2251443)

[2 АНТИФРОД — СИСТЕМЫ 7](#_Toc2251444)

[ЗАКЛЮЧЕНИЕ 9](#_Toc2251445)

[Список использованных источников 10](#_Toc2251446)

# ВВЕДЕНИЕ

В настоящее время дистанционное банковское обслуживание (далее — ДБО) является неотъемлемой частью банковских услуг, востребованных клиентами и удобных для кредитных организаций. Количество пользователей систем ДБО неуклонно растёт, увеличивается число и объем операций. Одновременно возрастает и риск от мошеннических действий злоумышленников, пытающихся на волне роста популярности дистанционного банкинга похищать денежные средства в системах ДБО.

# 1 ПРОБЛЕМА МОШЕННИЧЕСТВА В СИСТЕМАХ ДБО

На сегодняшний день счета юридических лиц являются наиболее привлекательной целью для компьютерных мошенников, ведь одна удачная кража может принести им миллионы рублей, а ответственность за такие преступления в нашей стране пока что минимальна. Такая ситуация требует от финансовых организаций, которые заботятся о своих клиентах,  постоянного совершенствования системы безопасности своей системы Интернет-банкинга.

Вместе с тем, не существует средств защиты, которые одинаково хорошо подходят для всех категорий клиентов. Например, кроме уровня безопасности, для малых предприятий максимальное значение имеет стоимость решения, для корпораций – скорость подписания транзакций, для VIP-клиентов – мобильность.

По оценкам экспертов, общий объем потерь клиентов систем дистанционного банкинга от хакерских атак на территории СНГ каждый год растет примерно на 80% и в 2018г. приблизится к 2 млрд. долларов.

Основной причиной проблемы в данном случае является невозможность (либо крайне высокая стоимость) создания доверенной рабочей среды на компьютере каждого клиента, что приводит к успешным реализациям атак на расчетные счета клиентов.  
Даже аппаратные средства криптографической защиты информации с неизвлекаемым ключом электронной подписи (ЭП) не позволяют надежно защитить  пользователей от современных видов атак.

Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от внесения изменений и замены, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи. ЭЦП обеспечивает:

• проверку целостности документов;

• конфиденциальность документов;

• установление лица, отправившего документ.

При проведении финансово значимых транзакций в системах дистанционного банковского обслуживания (ДБО), необходим контроль целостности подписываемого документа и подтверждение авторства. Современные технологии позволяют делать это при помощи электронной цифровой подписи (ЭЦП). В этом случае самым уязвимым звеном системы становится закрытый (секретный) ключ ЭЦП. Обеспечить его защиту от копирования можно, используя токены или смарт-карты с аппаратно реализованными криптографическими функциями. При этом закрытый ключ ЭЦП генерируется в смарт-карте, является неизвлекаемым и используется только для подписи передаваемых «снаружи» данных.

Однако, даже в случае использования аппаратных криптосредств, у злоумышленников остаются возможности для проведения мошеннических операций при помощи несанкционированного доступа к криптографическим возможностям смарт-карты или удаленного управления рабочей станцией пользователя. Причиной тому является невозможность построения доверенной среды на компьютерах клиентов, так как современные операционные системы (ОС) подвержены воздействию вредоносного программного обеспечения (вирусы, «трояны» и т.д.). Отдельно стоит отметить технологию «руткитов», которые перехватывают управление компьютером еще до загрузки операционной системы и не могут быть обнаружены классическими антивирусными средствами.

**Хищение ключей электронной подписи (ЭП) с незащищенных носителей.**

Наиболее простая и отработанная технология, при помощи которой до сих пор реализуется большинство атак на клиентов систем ДБО, хранящих ключи ЭП на флешках, дисках, дискетах, на жестком диске и т. д.

**Хищение закрытых ключей ЭП из оперативной памяти.**

Обычно применяется в случае использования клиентом средства защищенного хранения ключей ЭП, которое позволяет извлекать их из закрытой области памяти устройства.

**Несанкционированный доступ к криптографическим возможностям смарт-карты.**

Одна из наиболее опасных и перспективных атак. Реализуется либо при помощи средств удаленного управления компьютером клиента (класса TeamViewer), либо с использованием удаленного подключения к USB-порту (технология USB-over-IP). Ограничением для данной атаки является обязательное подключение смарт-карты (токена) в момент ее проведения.

**Подмена документа при передаче его на подпись в смарт-карту.**

Наиболее сложный и опасный на сегодняшний день вид атак. В данном случае пользователь видит на экране монитора одну информацию, а в смарт-карту на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях и т. д.

Таким образом, очевидно, что традиционных средств защиты, не позволяющих контролировать содержание подписываемого документа, на сегодняшний день недостаточно для защиты от современных видов атак.

Резко выросло количество вредоносного ПО для ПК, причем антивирусные средства не помогают, «кражи» SMS с мобильных устройств. Наряду с традиционными методами атак, такими, как фишинг, социальная инженерия, удаленный доступ, появляются новые методы, например, автоматическая подмена платежных реквизитов и виртуальные базовые станции мобильных операторов.

Против комбинаций этих методов традиционные методы защиты (SMS, генераторы одноразовых паролей, скретч-карты, традиционные антифрод-системы и пр.) становятся недостаточно эффективными:

**СМС/PUSH**

* Не привязана к реквизитам;
* Код подтверждения знает третья сторона: (Банк, Оператор / Apple&Google);
* Легко перехватывается;
* «Слабая» юридическая значимость;
* ДОРОГО.

**USB – токен**

* Всегда нужно иметь с собой;
* Не видно, что подписывается;
* Сложность логистики;
* ДОРОГО;
* Не может быть полноценно использован в мобильном устройстве (телефон, планшет, ультра-буки).

Киберпреступники хорошо оснащены и организованы, в таких группах есть ролевое распределение – координаторы, дропперы и прочие специализации. Технологии хищения также развиваются и представляют полноценный технологический процесс - от стадии выявления уязвимостей до готовых инструментов и методов хищения.

Атаки, при этом, могут вестись на информационные системы и самих банков и их клиентов, включая АРМ КБР (Автоматизированное рабочее место клиента Банка России), С[ДБО](http://www.tadviser.ru/index.php/%D0%94%D0%91%D0%9E) (система дистанционного банковского обслуживания), АБС (Автоматизированная банковская система) и прочие. Основная цель киберпреступников – максимизация прибыли от хищения при минимизации рисков, реже – причинение репутационного ущерба.

Как показывает практика, решение проблемы обеспечения безопасного дистанционного банковского обслуживания клиентов заключается в комплексном подходе, в сочетании организационных и технических средств защиты, как на стороне клиента, так и на стороне банка. В качестве распространённых и хорошо зарекомендовавших себя методов можно назвать использование на стороне клиента средств аутентификации (токены, считыватель смарт-карт Safe Touch, носители и генераторы сеансовых ключей), ограничение доступа (IP/MAC фильтрация), а на стороне банка — внедрение системы уведомления о событиях, автоматическое завершение по таймауту сессии пользователя, установка лимитов платежей, и т. п.

При этом полностью проблему мошенничества в системах ДБО невозможно решить исключительно техническими и организационными мерами — на каждую доработку систем защиты, на каждое организационное ограничение свободы работы клиента в системе ДБО всегда найдётся новое вредоносное программное обеспечение, новая техническая возможность мошенничества. Не секрет, что по-прежнему самой распространённой предпосылкой успешных атак является невыполнение пользователями основных рекомендаций по обеспечению безопасности при использовании операционной системы и, в частности, при работе в системе ДБО. Любые технические и программные средства будут бесполезны без соблюдения элементарных правил безопасности, без организационных мер. Хороший тому пример – рост числа хищений с помощью методов социального инжиниринга, когда человеческий фактор становится самым слабым звеном в цепи, против которых иногда бессильны самые продвинутые организационные и технические средства. С помощью этого метода происходит более 90% хищений денежных средств[[1]](#footnote-1).

# 2 АНТИФРОД — СИСТЕМЫ

Сегодня, по различным оценкам, порядка 95% краж средств клиентов банка связано с мошенничеством в интернет и мобильном банкинге. Природа мошенничества динамична, и каждый день появляются новые мошеннические схемы.

Современные системы дистанционного банковского обслуживания используют большое количество разнообразных антифрод-систем[[2]](#footnote-2), основной задачей которых является предотвращение осуществления подозрительных платежных поручений клиента. Большинство таких систем учитывают различные параметры платежного поручения в совокупности с некоторыми данными, полученными от клиента.

C помощью антифрод-систем фиксируются аномалии в поведении клиента и выявляются операции, имеющие признаки выполнения их не клиентами банка, а злоумышленниками.

Первоначально внедрение системы антифрода давало прорывной эффект в борьбе с мошенничеством: обнаруживались практически все платежи, созданные не на устройстве клиента. Однако мошенники адаптировались, и со временем всё больше платежей стало приходить непосредственно с устройств клиентов. Практически возможны только два способа выполнить подобное: либо произвести удаленное подключение к устройству клиента и выполнить платеж, либо произвести так называемую автозамену реквизитов платежа, создаваемого непосредственно клиентом. И то, и другое проходит не без помощи вирусного программного обеспечения.

Простейшие антифрод-решения используют обычные фильтры, аналогичные фильтрам в АБС (по сумме платежа, черным спискам и пр.), более сложные обучаются на накапливаемых данных о поведении клиентов, истории платежей и используют хорошо зарекомендовавшие себя методы машинного обучения, такие как поиск аномалий (отклонений от обычного поведения).

Все эти решения помимо их предназначения объединяет одно – они получают данные для анализа из некоторого источника и на основе определенных критериев делают свое заключение, считать ли платеж правомочным или мошенническим. Основным источником данных для анализа является система ДБО, т.к. именно через нее идет общение клиента с банком и именно в ней формируются платежные документы и другие события, анализом которых и занимается антифрод-система. Часть этих данных антифрод может получить и из АБС, но информация о многих событиях системы [ДБО](http://www.tadviser.ru/index.php/%D0%94%D0%91%D0%9E) до [АБС](http://www.tadviser.ru/index.php/%D0%90%D0%91%D0%A1) не доходит, т.к. в АБС она просто не нужна.

Также источниками информации могут служить «черные списки», распространяемые анти-дроп клубом, [ЦБ РФ](http://www.tadviser.ru/index.php/%D0%A6%D0%91_%D0%A0%D0%A4) ([FinCERT](http://www.tadviser.ru/index.php/FinCERT" \o "FinCERT)), базы проверки контрагентов, сформированные по открытым и закрытым источникам (например, от компании «Интегрум»).

Среди анализируемых антифрод-системой параметров и событий могут быть как данные о получателе платежа, банке получателя, назначении и сумме платежа, времени и периодичности платежей, остатке по счету, так и характеристики рабочего места отправителя платежа. Эти данные включают, в том числе, информацию о IP и MAC адресе, ошибках входа и изменения логина/пароля, изменении устройства, провайдера или домена в ходе сессии работы пользователя, наличии возможности для удаленного доступа, наличии обращений к зловредным доменам, файлах cookie, геоданных и прочие. В реально работающих системах фрод-анализа таких параметров десятки.

Как отмечалось выше, в развитых антифрод-системах данные анализируются в динамике, с учетом накапливаемой истории платежей по каждому клиенту и при каждом платеже или другом событии производится поиск аномалий, т.е. отклонений от стандартных паттернов поведения, присущих определенному клиенту.

Основными метриками эффективности антифрод-систем является процент ложных срабатываний – положительных (правомочный платеж признан фродом) и отрицательных (пропущен фродовый платеж). Обе метрики должны быть минимизированы, т.к. в случае положительного ложного срабатывания потребуется ручная проверка платежа (нагрузка на сотрудников банка) и до получателя деньги дойдут позже, а в случае отрицательного деньги будут украдены киберпреступниками. Эти две метрики взаимосвязаны и зависят от настройки чувствительности системы или, по-другому, от порога срабатывания. Развитые антифрод-системы при соответствующей настройке и опытном фрод-аналитике позволяют снизить положительные ложные срабатывания до менее 1%, а отрицательные свести практически к 0.

# ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в банках – задача, которая никогда не может быть решена полностью на 100%, поскольку киберпреступники неустанно ищут новые инструменты и подходы для того, чтобы похищать либо средства со счетов банковских организаций, либо деньги со счетов банковских клиентов. Улучшения систем информационной безопасности, даже если они есть, носят временный характер, а мошенники не исчезают, и, более того, они демонстрируют гибкость в своих подходах, постоянно меняют цели и инструменты их достижения. А также киберпреступники в некотором смысле даже преподнесли банковскому сообществу урок, очень быстро наладив эффективное взаимодействие между собой, постоянный обмен информацией об исходных кодах, уязвимостях банковских систем и т.д.

Недавно вышло постановление ЦБ, которое требует не только передавать информацию о сомнительных платежах в Росфинмониторинг, но и останавливать их. В частности, была внесена принципиальная правка — если банкам раньше предоставлялось право блокировать подозрительные переводы, тогда как сейчас это вменяется им в обязанность. Таким образом, Банки будут обязаны блокировать операции по переводу денег на срок до двух дней, если транзакция покажется им подозрительной, т.е. сработает система обнаружения мошеннических операций. Однако, не смотря на то, что решение проблем обеспечения информационной безопасности Банки берут на себя, главная задача — это научить самих пользователей систем ДБО управлять рисками, которые сопровождают развитие цифровых финансовых услуг.

# Список использованных источников

1. Атаки на системы ДБО [Электронный ресурс]. URL: <https://www.securitylab.ru/analytics/485467.php>
2. Анти-фрод системы и как они работают [Электронный ресурс]. URL: <https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/339929.php>
3. Безопасность ДБО [Электронный ресурс]. URL: <http://bankir.ru/publikacii/20120604/bezopasnost-dbo-zavisit-i-ot-banka-i-ot-klienta-10001755/>
4. Безопасность систем дистанционного банковского обслуживания [Электронный ресурс]. URL: <http://bankir.ru/publikacii/20120305/bezopasnost-sistem-distantsionnogo-bankovskogo-obsluzhivaniya-10001328/>
5. Безопасность [Электронный ресурс]. URL: <http://www.bankdbo.ru/bezopasnost>
6. Что умеет ANTI-FRAUD в ДБО? [Электронный ресурс]. URL:  
   <http://www.bssys.com/about/press-center/articles/chto-umeet-anti-fraud-v-dbo/>
7. FRAUD-Анализ [Электронный ресурс]. URL: <http://www.bssys.com/solutions/financial-institutions/fraud/>
8. Как выбрать антифрод-систему для банка? [Электронный ресурс]. URL: <http://www.tadviser.ru/index.php/Статья:Как_выбрать_антифрод-систему_для_банка>

1. По данным издания «[Российская газета» - Федеральный выпуск №7122 (254)](https://rg.ru/gazeta/rg/2016/11/10.html) от 10 ноября 2016 г. [↑](#footnote-ref-1)
2. Термин «фрод» произошел от английского слова «fraud», что переводится как «мошенничество» [↑](#footnote-ref-2)