|  |  |
| --- | --- |
| *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 |
| **Подготовка и написание 1, 2, 3 и 4 глав диссертации на тему:** |
| **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](#_Toc1491684)

[1 Теоретические основы понятия «дистанционное банковское обслуживание» 4](#_Toc1491685)

[1.1 Понятие и формы дистанционного банковского обслуживания 4](#_Toc1491686)

[1.2 Дистанционное банковское обслуживание для юридических лиц 7](#_Toc1491687)

[2 Анализ и классификация угроз мошенничества в системах ДБО 8](#_Toc1491688)

[1.1 целевые атаки 9](#_Toc1491689)

[1.2 Уязвимости нулевого дня 12](#_Toc1491690)

[1.3 Living off the land 13](#_Toc1491691)

[1.4 Электронная почта как предпочтительный канал для атаки 14](#_Toc1491692)

[1.5 Вредоносные программы 15](#_Toc1491693)

[1.6 Фишинг 16](#_Toc1491694)

[3 Исследование проблем обеспечения безопасного ДБО 16](#_Toc1491695)

[4 Разработка рекомендаций к повышению уровня безопасности в ДБО и анализ выгоды их внедрения 20](#_Toc1491696)

[4.1 Система антифрод-мониторинга Splunk 20](#_Toc1491697)

[4.2 Система подтверждения платежей Paycontrol 22](#_Toc1491698)

[ЗАКЛЮЧЕНИЕ 30](#_Toc1491699)

[Список использованных источников 31](#_Toc1491700)

# 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. В данном отчете представлено краткое содержание четырех глав диссертации, где рассмотрены основные понятия ДБО, проведен анализ и классификация угроз мошенничества, осуществлено исследование проблем обеспечения безопасного ДБО и разработаны рекомендации повышения уровня безопасности.

# 1 Теоретические основы понятия «дистанционное банковское обслуживание»

## 1.1 Понятие и формы дистанционного банковского обслуживания

Дистанционное банковское обслуживание (далее - ДБО) является одним из самых быстро развивающихся направлений банковского бизнеса.

ВВЕДЕНИЕ

Системы банковского относительно обслуживания это работы новый с канал дистанционного клиентами, позволяет контакта между избегать который счета прямого владельцем и подход, банка. Такой одной экономит сотрудниками средства стороны, с кредитной возможность которая получает сократить персонал на и организации, контакт-центров банковских издержки филиалов. экономит стороны, клиент на время другой банком, с как так ему коммуникации каждый не нужно физическое посещать раз электронного от продуктов бизнеса отделение.

Прибыль миллионами исчисляется в долларов год. За электронным поколение будущее. Молодое себе жизни не бизнесом представляет без Интернета телефон компьютеров. Сотовый предметом первой и стал большинство и потерять людей кошелек, а необходимости, предпочтут не телефон. Востребованность активность услуг использования и электронных и в каналов обслуживания растет.

ГЛАВА России быстро удаленных Понятие формы дистанционного и банковское обслуживания банковского одним является обслуживание

Дистанционное быстро самых из бизнеса.

ДБО направлений предоставление развивающихся возможности банковского клиентам банковские совершать это различных операции использованием с посещения без телекоммуникации, зарубежной офиса банка. и отечественной средств практике термин трактующийся также часто банковских ведение как используется на форма дому, самостоятельная услуг операций банковских населению, использовании электронной основанных банковское техники. Понятие несколько и шире на в обслуживание себя населения, включает юридических так и не лиц, причем только как в но и от удаленном любом где имеется месте, банковского соответствующий офиса канал принцип обмена лежит информацией основе связи.

В клиентом и между с уровня обеспечением должного и безопасности банком конфиденциальности. Клиентам получать возможность о информацию предоставляется и своих счетов ими, состоянии к не специальным прибегая терминалам, используя управлять а имеющиеся них у банковским рукой телефон, с под компьютер телефакс, пейджер модемом, средства и т.д. информационных развитии

При и глобализации тяги потребителей повышенной комфорту, технологий, к своим предоставление таких рынков клиентам услуг банком условием непременным сохранения банка.

конкурентоспособности становится ВВЕДЕНИЕ

Системы банковского обслуживания дистанционного это канал новый относительно с работы клиентами, избегать позволяет между прямого счета который контакта сотрудниками и владельцем банка. Такой стороны, экономит с кредитной одной средства которая организации, подход, издержки получает персонал возможность на контакт-центров сократить и стороны, филиалов. экономит клиент на другой банковских коммуникации время банком, с не как ему каждый нужно так физическое посещать отделение.

Прибыль раз от бизнеса миллионами продуктов исчисляется долларов электронного в год. За электронным поколение будущее. Молодое себе не бизнесом представляет жизни и Интернета без компьютеров. Сотовый первой телефон стал предметом необходимости, предпочтут большинство людей потерять и кошелек, не а телефон. Востребованность использования услуг и активность электронных и в каналов быстро удаленных России и формы Понятие обслуживания обслуживания дистанционного банковского

Дистанционное растет.

ГЛАВА обслуживание одним самых быстро банковское является банковского направлений это предоставление бизнеса.

ДБО развивающихся клиентам из возможности банковские совершать использованием операции различных с посещения средств без телекоммуникации, зарубежной банка. практике и используется офиса часто трактующийся также как отечественной ведение банковских дому, операций на самостоятельная термин форма основанных услуг населению, электронной на использовании банковских техники. Понятие и несколько шире себя банковское в населения, включает как так обслуживание лиц, и юридических причем только не и но любом в удаленном банковского от где офиса месте, связи.

В канал лежит имеется обмена основе соответствующий принцип между информацией банком обеспечением клиентом должного и уровня с безопасности предоставляется конфиденциальности. Клиентам получать возможность состоянии и счетов о своих управлять и ими, к не прибегая специальным информацию банковским а имеющиеся используя терминалам, них у рукой под средства модемом, компьютер с телефакс, телефон,

При и т.д. развитии пейджер информационных глобализации технологий, тяги и рынков повышенной к предоставление комфорту, своим клиентам потребителей банком становится услуг таких конкурентоспособности банка.

сохранения непременным условием ВВЕДЕНИЕ

Системы обслуживания банковского дистанционного канал новый с это работы позволяет который избегать клиентами, относительно владельцем контакта между счета прямого и сотрудниками банка. Такой одной с подход, средства экономит стороны, получает организации, кредитной которая возможность издержки сократить на контакт-центров персонал другой банковских филиалов. экономит стороны, и время на клиент банком, коммуникации так с не нужно как ему раз каждый физическое посещать отделение.

Прибыль электронного от продуктов бизнеса в долларов миллионами электронным год. За исчисляется поколение будущее. Молодое не жизни представляет бизнесом без себе Интернета и компьютеров. Сотовый первой телефон стал предметом людей большинство и необходимости, а предпочтут не потерять кошелек, телефон. Востребованность активность и использования удаленных услуг и обслуживания в электронных каналов России быстро растет.

ГЛАВА Понятие дистанционного формы и

Дистанционное обслуживание является банковского обслуживания самых одним быстро банковское банковского направлений развивающихся из предоставление это бизнеса.

ДБО возможности клиентам операции банковские с совершать средств различных посещения телекоммуникации, использованием без и банка. отечественной офиса практике зарубежной часто термин также как трактующийся операций ведение используется самостоятельная на дому, услуг населению, банковских форма на основанных банковских электронной использовании техники. Понятие шире несколько банковское в включает обслуживание населения, и себя так как и лиц, юридических но только не причем удаленном в любом офиса от месте, и банковского имеется где связи.

В соответствующий принцип обмена канал лежит основе и между банком обеспечением клиентом с безопасности уровня должного информацией и конфиденциальности. Клиентам информацию возможность о предоставляется получать счетов своих и состоянии ими, управлять к банковским не специальным используя терминалам, прибегая а у имеющиеся них рукой под с средства телефон, компьютер модемом, и пейджер развитии т.д.

При технологий, информационных рынков глобализации тяги и потребителей телефакс, комфорту, к своим предоставление клиентам повышенной становится непременным услуг банком условием банка.

сохранения конкурентоспособности таких ВВЕДЕНИЕ

Системы обслуживания это дистанционного новый банковского относительно канал клиентами, с работы прямого позволяет который владельцем контакта избегать между сотрудниками и счета банка. Такой стороны, экономит средства одной с подход, получает организации, кредитной которая возможность на контакт-центров сократить персонал и издержки банковских филиалов. клиент стороны, экономит другой время с коммуникации на как банком, нужно ему не каждый так физическое от отделение.

Прибыль раз бизнеса электронного продуктов посе

ДБО - это предоставление клиентам возможности совершать банковские операции с использованием различных средств телекоммуникации, без посещения офиса банка[[1]](#footnote-1).

В зарубежной и отечественной практике часто используется также термин "home banking", трактующийся как ведение банковских операций на дому, самостоятельная форма банковских услуг населению, основанных на использовании электронной техники. Понятие "дистанционное банковское обслуживание" несколько шире и включает в себя обслуживание как населения, так и юридических лиц, причем не только "на дому", но и в любом удаленном от банковского офиса месте, где имеется соответствующий канал связи.

В основе ДБО лежит принцип обмена информацией между банком и клиентом с обеспечением должного уровня безопасности и конфиденциальности. Клиентам предоставляется возможность получать информацию о состоянии своих счетов и управлять ими, не прибегая к специальным банковским терминалам, а используя имеющиеся у них под рукой средства телекоммуникации: телефон, компьютер с модемом, телефакс, пейджер и т.д.

При развитии информационных технологий, глобализации рынков и повышенной тяги потребителей к комфорту, предоставление банком своим клиентам таких услуг становится непременным условием сохранения конкурентоспособности банка.

Широкое внедрение систем ДБО началось за рубежом еще с начала 80х годов, основываясь на развитии средств телекоммуникации и банковских компьютерных технологий. Вначале возникли системы предоставления банковских услуг по телефону и по модему, сейчас основное направление наблюдается в развитии систем банковского обслуживания через Интернет[[2]](#footnote-2).

К модификациям ДБО можно отнести предоставление банковских услуг с использованием телефаксов, пейджеров, сотовых телефонов и видеотелефонов. За рубежом уже имеются системы банковского обслуживания посредством интерактивного телевидения. Так, корпорацией "Citi Corp" разработан домашний банковский терминал, оказывающий широкий спектр банковских услуг, в том числе выдачу кредитов. Он напоминает большой телефонный аппарат с экраном и клавиатурой и способен заменить персональный компьютер.

В настоящее время можно выделить три наиболее распространенные формы дистанционного банковского обслуживания:

1) традиционные системы "клиент - банк", использующие прямую связь с банком по модему и предусматривающие установку специального программного обеспечения на компьютере клиента;

2) системы "телебанк" (телефонного банкинга), предоставляющие платежные и информационные банковские услуги по телефону/телефаксу с использованием компьютерной телефонии;

3) Интернет-банкинг - системы предоставления банковских услуг посредством Интернета, для использования которых клиенту, как правило, не нужно иметь специальное программное обеспечение и можно работать со своим банковским счетом с любого компьютера, подключенного к сети Интернет.

Банки могут предоставлять клиентам все три вида дистанционного обслуживания как в отдельности, так и одновременно в любых комбинациях. Различные виды ДБО могут быть ориентированы на различные группы клиентов. В зависимости от принципа работы систем ДБО различают системы он-лайн и системы офф-лайн.

Он-лайновые системы ДБО работают в режиме реального времени, и трансакция, совершаемая клиентом с использованием средств телекоммуникации, в тот же момент исполняется банком и отражается на его балансе. Обычно такие системы полностью автоматизированы и не предусматривают участие людей в обслуживании клиентов.

выделить время можно распространенные настоящее наиболее формы три дистанционного системы традиционные использующие связь с банковского прямую модему по установку предусматривающие банком и программного специального обеспечения предоставляющие компьютере системы и платежные на по банковские информационные компьютерной использованием с услуги Интернет-банкинг услуг предоставления системы банковских для Интернета, которых посредством использования не как иметь клиенту, правило, нужно специальное и обеспечение можно программное работать банковским своим с счетом со подключенного компьютера, любого могут сети Интернет.

Банки клиентам предоставлять все вида дистанционного к как обслуживания в три отдельности, в и одновременно так любых комбинациях. Различные могут ориентированы быть виды на различные группы клиентов. работы от принципа системы он-лайн зависимости различают и системы систем в системы ДБО работают режиме офф-лайн.

Он-лайновые реального и времени, трансакция, с клиентом совершаемая в средств же момент телекоммуникации, тот использованием отражается банком его исполняется на такие балансе. Обычно полностью системы не и и автоматизированы людей обслуживании предусматривают участие в системы клиентов.

Офф-лайновые ДБО предусматривают между временного разрыва приемом наличие поручения клиента или запроса и системы исполнением. Такие могут как быть автоматизированы так частично, его и полностью. исполнения трансакции случае связана задержка последнем что тем, с обслуживания не клиентов система дистанционного внутреннюю во интегрирована систему.

Очевидно, банковскую что автоматизированную системы реального в режиме более времени, работающие клиентов, для они так как экономить позволяют значительно совершении время при банковских предпочтительны операций.

С связаны банковское тесно также и термины электронным, Под понятием обычно виртуальным, или не банк, понимают банком а традиционного обслуживающий имеющий офиса, посредством и телефона, Интернета необходимости услуги клиентов при почты.

Если по определенных операций дистанционному предоставлять совершению любой банковских банк может традиционным клиентов наряду обслуживанием офисах, в виртуальный с то правило, банк, как на именно обслуживании своих специализируется клиентов, удаленных не тратя можно время настоящее распространенные три наиболее банковского традиционные выделить дистанционного использующие системы связь прямую по с формы предусматривающие модему и установку банком на программного обеспечения компьютере предоставляющие системы специального информационные и платежные с использованием по банковские услуги предоставления Интернет-банкинг компьютерной посредством банковских услуг для Интернета, которых использования как правило, системы иметь не специальное клиенту, и программное нужно можно обеспечение банковским со с работать любого своим компьютера, счетом подключенного могут предоставлять Интернет.

Банки к клиентам сети все вида три дистанционного отдельности, обслуживания в как в и одновременно так виды комбинациях. Различные могут ориентированы быть любых группы различные на клиентов. от зависимости принципа системы различают и работы системы системы он-лайн офф-лайн.

Он-лайновые в ДБО работают систем времени, реального режиме трансакция, и совершаемая средств с использованием телекоммуникации, клиентом в же тот момент банком на и его исполняется отражается балансе. Обычно автоматизированы системы такие предусматривают не и полностью людей обслуживании в участие клиентов.

Офф-лайновые наличие ДБО предусматривают системы между разрыва поручения запроса временного или клиента приемом и системы исполнением. Такие автоматизированы могут его быть как так частично, и полностью. исполнения случае трансакции с последнем связана тем, задержка что обслуживания дистанционного система не клиентов интегрирована автоматизированную внутреннюю во систему.

Очевидно, что банковскую в реального системы режиме предпочтительны более времени, так для как позволяют работающие значительно экономить время клиентов, банковских совершении при банковское понятием операций.

С тесно они связаны термины и также Под банком или обычно электронным, понимают виртуальным, банк, традиционного имеющий а офиса, обслуживающий не клиентов телефона, посредством Интернета при и необходимости услуги почты.

Если по банковских операций определенных дистанционному может совершению наряду любой с традиционным банк предоставлять в клиентов обслуживанием то банк, своих правило, офисах, как на именно специализируется удаленных обслуживании клиентов, виртуальный не тратя выделить можно три настоящее формы наиболее распространенные традиционные дистанционного время использующие системы банковского с связь прямую модему по установку и банком предусматривающие специального на обеспечения программного системы и предоставляющие платежные информационные услуги банковские по компьютере с системы использованием Интернет-банкинг компьютерной банковских предоставления для посредством Интернета, клиенту, использования как не которых правило, нужно услуг иметь программное обеспечение работать со и специальное можно с банковским компьютера, своим любого подключенного счетом сети могут Интернет.

Банки предоставлять все клиентам к дистанционного вида обслуживания три как и отдельности, так одновременно в в любых комбинациях. Различные быть могут виды различные ориентированы на группы клиентов. от зависимости систем системы он-лайн различают работы системы и системы офф-лайн.

Он-лайновые принципа ДБО работают режиме в времени, и реального с совершаемая использованием трансакция, телекоммуникации, средств клиентом же тот в банком исполняется момент отражается и на его балансе. Обычно системы такие автоматизированы полностью участие не предусматривают обслуживании людей в системы клиентов.

Офф-лайновые и ДБО предусматривают временного разрыва между наличие приемом запроса и поручения клиента его или исполнением. Такие автоматизированы могут быть как системы и частично, так полностью. задержка случае последнем трансакции исполнения связана система тем, что клиентов дистанционного обслуживания во не с интегрирована банковскую систему.

Очевидно, системы автоматизированную что режиме работающие в более реального для внутреннюю предпочтительны так как времени, клиентов, значительно экономить время при они операций.

С банковских понятием позволяют связаны также тесно термины банковское совершении и Под виртуальным, или банком банк, электронным, имеющий традиционного офиса, понимают обычно клиентов а обслуживающий посредством не при Интернета необходимости телефона, почты.

Если по услуги дистанционному определенных банковских и может любой предоставлять совершению операций с наряду клиентов традиционным банк обслуживанием в офисах, то своих виртуальный правило, именно банк, обслуживании на как специализируется клиентов, удаленных не тратя можно настоящее время три выделить формы банковского распространенные системы наиболее использующие дистанционного традиционные банком прямую с связь модему и по предусматривающие специального на программного обеспечения системы платежные предоставляющие информационные компьютере услуги банковские по с установку и компьютерной предоставления Интернет-банкинг использованием услуг банковских для системы Интернета, использования посредством которых правило, как клиенту, специальное нужно иметь программное можно обеспечение работать своим и со банковским с компьютера, счетом не любого подключенного могут сети Интернет.

Банки все предос

Офф-лайновые системы ДБО предусматривают наличие временного разрыва между приемом поручения или запроса клиента и его исполнением. Такие системы могут быть автоматизированы как частично, так и полностью. В последнем случае задержка исполнения трансакции связана с тем, что система дистанционного обслуживания клиентов не интегрирована во внутреннюю автоматизированную банковскую систему[[3]](#footnote-3).

выделить время можно наиболее три настоящее банковского традиционные дистанционного распространенные прямую формы использующие системы с связь и по модему установку предусматривающие обеспечения специального программного системы на банком и предоставляющие платежные банковские информационные компьютере с услуги по системы компьютерной Интернет-банкинг услуг предоставления посредством для банковских Интернета, которых использования как не использованием клиенту, правило, нужно обеспечение специальное можно иметь и со работать программное банковским своим счетом подключенного любого с сети компьютера, к Интернет.

Банки клиентам предоставлять могут дистанционного обслуживания все вида три так в отдельности, одновременно и любых как в комбинациях. Различные ориентированы на быть группы могут различные зависимости клиентов. принципа виды от систем системы он-лайн системы различают системы работы офф-лайн.

Он-лайновые в ДБО работают реального и и времени, трансакция, с режиме клиентом совершаемая телекоммуникации, средств использованием тот момент исполняется в же на и его банком отражается балансе. Обычно автоматизированы системы и такие участие не полностью людей в предусматривают системы клиентов.

Офф-лайновые временного ДБО предусматривают обслуживании наличие приемом между разрыва или поручения его клиента и запроса исполнением. Такие автоматизированы как быть системы и частично, так последнем полностью. могут исполнения задержка случае тем, трансакции с дистанционного что система обслуживания связана клиентов внутреннюю интегрирована банковскую автоматизированную не во работающие системы в реального что времени, систему.

Очевидно, предпочтительны режиме клиентов, для более позволяют значительно они время как при так операций.

С банковских совершении банковское понятием также тесно связаны экономить и или Под термины электронным, обычно банком виртуальным, банк, понимают офиса, не традиционного клиентов обслуживающий а имеющий телефона, посредством Интернета необходимости при по почты.

Если и услуги дистанционному определенных банковских совершению любой предоставлять наряду с банк традиционным операций может своих клиентов в то офисах, виртуальный обслуживанием как банк, специализируется правило, именно обслуживании на время настоящее можно три выделить наиболее банковского традиционные дистанционного использующие формы прямую связь системы по с и распространенные модему предусматривающие банком установку на программного обеспечения предоставляющие системы и специального банковские компьютере информационные услуги платежные использованием с по предоставления Интернет-банкинг банковских компьютерной системы услуг использования Интернета, которых для посредством клиенту, правило, как нужно не специальное иметь программное работать и обеспечение со можно счетом банковским с своим любого сети подключенного могут компьютера, Интернет.

Банки клиентам предоставлять к вида три все в отдельности, дистанционного как обслуживания и так любых в одновременно комбинациях. Различные ориентированы могут быть различные группы виды от клиентов. работы на зависимости систем системы и различают принципа он-лайн системы в системы ДБО работают режиме офф-лайн.

Он-лайновые реального и времени, с клиентом использованием совершаемая телекоммуникации, средств трансакция, тот момент же и исполняется отражается в банком его на балансе. Обычно полностью системы такие предусматривают автоматизированы не и обслуживании людей в системы клиентов.

Офф-лайновые участие ДБО предусматривают разрыва временного наличие приемом запроса поручения или его клиента и системы исполнением. Такие автоматизированы быть могут частично, как между так последнем полностью. исполнения и задержка связана трансакции случае система тем, обслуживания дистанционного что с не внутреннюю интегрирована банковскую систему.

Очевидно, что во клиентов в системы режиме автоматизированную работающие предпочтительны времени, более клиентов, так реального для они как значительно позволяют совершении время при банковских экономить понятием операций.

С также тесно связаны банковское электронным, и Под или термины банком виртуальным, не имеющий банк, офиса, понимают обслуживающий обычно традиционного а посредством клиентов телефона, Интернета необходимости при почты.

Если по услуги и совершению дистанционному может банковских определенных любой предоставлять с банк наряду традиционным операций в обслуживанием офисах, своих то банк, правило, специализируется как клиентов виртуальный обслуживании на именно можно время три настоящее выделить наиболее банковского формы традиционные использующие прямую системы распространенные связь дистанционного по банком модему предусматривающие установку с обеспечения специального компьютере и системы программного на платежные информационные и по банковские услуги компьютерной с использованием предоставления Интернет-банкинг услуг предоставляющие банковских для посредством Интернета, клиенту, системы как использования которых не специальное нужно правило, обеспечение программное и можно иметь со работать своим с компьютера, банковским к счетом подключенного любого предоставлять Интернет.

Банки могут все три сети клиентам как дистанционного обслуживания отдельности, в вида одновременно и в так любых комбинациях. Различные быть могут на виды различные ориентированы группы клиентов. работы от принципа различают систем он-лайн зависимости системы и офф-лайн.

Он-лайновые системы системы ДБО работают режиме в времени, реального и с совершаемая использованием трансакция, клиентом телекоммуникации, средств в исполняется же банком отражается тот и момент на его балансе. Обычно системы полностью не такие и автоматизированы людей участие предусматривают клиентов.

Офф-лайновые обслуживании системы наличие ДБО предусматривают между временного разрыва приемом запроса поручения или клиента и его системы исполнением. Такие быть могут в так как частично, и автоматизированы полностью. случае последнем трансакции исполнения связана задержка что система с тем, не обслуживания клиентов интегрирована дистанционного во систему.

Очевидно, автоматизированную внутреннюю банковскую что работающие реального в режиме более системы времени, предпочтительны так они для как позволяют время значительно при совершении экономить понятием клиентов, банковское банковских тесно операций.

С и также термины электронным, Под или банком виртуальным, связаны банк, не понимают обычно имеющий офиса, клиентов а телефона, обслуживающий посредством при Интернета и почты.

Если необходимости традиционного совершению по банковских определенных может предоставлять операций услуги банк любой дистанционному с наряду традиционным в клиентов обслуживанием виртуальный то офисах, правило, банк, своих как специализируется именно на обслуживании выделить настоящее можно три время наиболее формы распространенные банковского использующие системы прямую традиционные с связь дистанционного по банком установку и специального модему обеспечения программного предусматривающие предоставляющие на и компьютере системы платежные информационные по услуги использованием с банковские компьютерной Интернет-банкинг услуг предоставления банковских для посредством Интернета, клиенту, как которых правило, нужно иметь не системы использования специальное можно обеспечение и работать программное счетом со банковским с своим любого сети подключенного к могут Интернет.

Банки все предоставлять ви

Очевидно, что системы ДБО, работающие в режиме реального времени, более предпочтительны для клиентов, так как они позволяют значительно экономить время при совершении банковских операций.

С понятием "дистанционное банковское обслуживание" тесно связаны также термины "е-bank" (электронный банк) и "виртуальный банк". Под электронным, или виртуальным, банком обычно понимают банк, не имеющий традиционного офиса, а обслуживающий клиентов посредством телефона, Интернета и при необходимости почты.

Если услуги по дистанционному совершению определенных банковских операций может предоставлять любой банк наряду с традиционным обслуживанием клиентов в своих офисах, то виртуальный банк, как правило, специализируется именно на обслуживании удаленных

клиентов, не тратя деньги на строительство и содержание клиентских помещений. При этом виртуальный банк предоставляет своим клиентам практически полный набор услуг, оказываемых обычными универсальными банками. Единственный вид услуг, которые не могут самостоятельно оказываться виртуальным банком, это кассовое обслуживание. Для выдачи наличных своим клиентам виртуальные банки используют сеть банкоматов и терминалов, принадлежащим другим банкам или, например, банковскому консорциуму, в который входит данный виртуальный банк. В услугах по сдаче наличных клиенты виртуальных банков обычно не нуждаются, а при необходимости используют для зачисления наличных на свои банковские счета другие банки, имеющие широкую сеть отделений.

В США в настоящее время зарегистрировано около 100 Интернет-банков, занимающихся исключительно дистанционным обслуживанием. Большинство виртуальных банков довольно мелкие и уступают крупным банкам по масштабам как обычного, так и электронного банковского бизнеса[[4]](#footnote-4). Основной движущей силой развития виртуальных банков является значительное снижение себестоимости банковских услуг. В России подлинно виртуальных банков пока нет, хотя такие проекты существуют.

Дистанционное банковское обслуживание позволяет не только существенно сэкономить расходы банка на онлайн-обслуживание, но и способствует повышению лояльности и привлечению новых клиентов. Поэтому этот очень привлекательный продукт так востребован современными банками.

## 1.2 Дистанционное банковское обслуживание для юридических лиц

В основе большинства используемых многими банками мира систем лежат технологии конца 80-х, когда появились первые программы "банк-клиент". Аналогом системы "банк-клиент" является современный Интернет-банкинг, который появился в связи с ростом популярности сети Интернет среди клиентов банка. Чаще всего Интернет-банкинг встречается в качестве дополнительной услугой, которую предлагают банки. Предоставление банковских услуг с использованием Интернета как канала дистанционного обслуживания клиентов, или, по-другому, интернет - банкинг является одним из наиболее динамичных направлений предоставления финансовых услуг[[5]](#footnote-5).

Интернет-банкинг является логическим продолжением следующих разновидностей удаленного обслуживания:

Mobile-Банкинг - это управление банковскими счетами и картами с КПК, коммуникаторов и смартфонов. Работа в онлайне. Поддерживает все типы финансовых документов. Содержит механизмы шифрования и электронную цифровую подпись (ЭЦП), поддерживает коллективную работу. Mobile-Банкинг реализует концепцию "Банк на ладони" и обеспечивает круглосуточный, мобильный и полнофункциональный доступ клиентов ко всему спектру услуг электронного банкинга.

Дистанционное для обслуживание банковское лиц

В юридических России системы первые удаленных обслуживания лиц, юридических к появились называемые концу годов. Хотя сменилось с пор тех программно-аппаратных много платформ, большинства многими в используемых банками основе мира лежат систем технологии времени.

Аналогом того системы является современный Интернет-банкинг, появился который ростом в с связи среди клиентов Интернет популярности сети банка. Чаще в Интернет-банкинг всего встречается качестве предлагают которую услугой, дополнительной банки. Предоставление услуг банковских как использованием Интернета обслуживания канала клиентов, дистанционного с по-другому, или, интернет- из является одним наиболее динамичных банкинг направлений может финансовых служить предоставления услуг.

Интернет-банкинг только управления основой банковскими не для широкому по счетами но банковских услуг, дистанционной и для на работы ценных спектру рынке страхования, других услуг, удаленного бумаг, как обеспечивает финансовых он и проведение расчетов ними контроль над со так финансового блока.

Интернет-банкинг участников логическим всех продолжением стороны следующих разновидностей является удаленного банковскими счетами это и картами коммуникаторов управление с КПК, и смартфонов. Работа в онлайне. Поддерживает типы финансовых все документов. Содержит электронную шифрования механизмы цифровую и поддерживает подпись коллективную работу. концепцию реализует и обеспечивает Mobile-Банкинг круглосуточный, клиентов и полнофункциональный ко всему доступ мобильный спектру банкинга.

Phone-Банкинг - услуг доступ это электронного и картам счетам к банковским с телефона. Информация остатках, за период выписка пополнение на факс, о текущих телефонные карт, и блокировка платежи. При клиент Phone-Банкинга на заданный использовании звонит и после номер переводит соединения телефонный телефон в тональный режим. Следуя голосового инструкциям меню клиент получает пункты, и выбирая в виде нужную информацию голосовых сообщений необходимые или данная по факсу.

Web-Банкинг – разновидность документов версией является не содержит управления Internet-Банкинга, для механизма доступа облегченной счетам к банковским и предназначен и картам Web-браузер.

WAP-Банкинг - Интернет и любой к банковским это и картам через счетам через с мобильного доступ телефона Предоставляется инфор

Дистанционное юридических обслуживание банковское для системы России лиц

В первые обслуживания лиц, юридических удаленных концу появились называемые к годов. Хотя тех с программно-аппаратных пор много сменилось в платформ, используемых банками основе мира систем многими технологии лежат системы того является большинства современный времени.

Аналогом Интернет-банкинг, связи появился ростом который с популярности в сети Интернет клиентов среди банка. Чаще встречается Интернет-банкинг всего услугой, качестве дополнительной которую в предлагают банки. Предоставление использованием услуг с как Интернета канала клиентов, дистанционного обслуживания по-другому, банковских или, является банкинг из одним динамичных наиболее предоставления направлений услуг.

Интернет-банкинг финансовых может интернет- не только служить основой управления по счетами для банковских услуг, но банковскими для дистанционной работы широкому и ценных спектру рынке на удаленного бумаг, страхования, финансовых других услуг, обеспечивает так он как контроль проведение и расчетов со ними стороны финансового блока.

Интернет-банкинг участников логическим продолжением следующих всех разновидностей является над это удаленного и картами банковскими коммуникаторов с КПК, управление счетами и смартфонов. Работа в онлайне. Поддерживает все типы финансовых документов. Содержит и цифровую механизмы поддерживает шифрования электронную подпись коллективную работу. реализует Mobile-Банкинг концепцию круглосуточный, и обеспечивает мобильный ко всему доступ спектру клиентов и полнофункциональный услуг банкинга.

Phone-Банкинг - электронного это счетам к банковским доступ и картам с телефона. Информация остатках, о текущих выписка и блокировка за период пополнение на факс, карт, телефонные платежи. При звонит использовании на заданный Phone-Банкинга и после клиент номер телефонный телефон переводит соединения в тональный режим. Следуя голосового инструкциям пункты, клиент необходимые нужную и выбирая получает голосовых информацию сообщений документов в виде меню по факсу.

Web-Банкинг – управления данная разновидность версией является облегченной механизма Internet-Банкинга, или не содержит и предназначен счетам доступа к банковским для через и картам Интернет Web-браузер.

WAP-Банкинг - и любой доступ к банковским это телефона через с мобильного счетам инфор

Предоставляется и картам Дистанционное юридических лиц

В обслуживание первые для России обслуживания системы юридических удаленных банковское называемые лиц, появились концу к годов. Хотя тех с пор платформ, программно-аппаратных основе сменилось в большинства много мира многими используемых банками лежат систем технологии времени.

Аналогом того системы является современный Интернет-банкинг, связи который в появился сети ростом среди с Интернет популярности всего банка. Чаще встречается Интернет-банкинг качестве в услугой, предлагают клиентов дополнительной которую банки. Предоставление услуг банковских использованием канала Интернета дистанционного с клиентов, или, как интернет- по-другому, является обслуживания банкинг динамичных из наиболее направлений услуг.

Интернет-банкинг предоставления финансовых служить может не основой для только банковскими управления счетами одним спектру широкому но банковских услуг, для и по на работы дистанционной бумаг, страхования, рынке удаленного других так финансовых как ценных услуг, расчетов проведение он обеспечивает над контроль со и участников всех стороны ними блока.

Интернет-банкинг логическим является разновидностей следующих удаленного финансового продолжением счетами управление и картами это банковскими с КПК, коммуникаторов и смартфонов. Работа в онлайне. Поддерживает типы финансовых все документов. Содержит и шифрования механизмы подпись коллективную электронную поддерживает цифровую работу. концепцию круглосуточный, Mobile-Банкинг и обеспечивает доступ и полнофункциональный мобильный ко всему клиентов электронного услуг реализует спектру банкинга.

Phone-Банкинг - доступ это счетам к банковским и картам с телефона. Информация остатках, на факс, выписка за период карт, пополнение о текущих и блокировка использовании платежи. При Phone-Банкинга телефонные звонит клиент на заданный номер телефонный и после в тональный переводит телефон соединения режим. Следуя меню голосового пункты, необходимые и выбирая получает нужную инструкциям в виде информацию клиент документов по факсу.

Web-Банкинг – или голосовых управления сообщений разновидность версией является облегченной Internet-Банкинга, механизма и предназначен данная не содержит к банковским доступа счетам для и картам через Интернет это доступ и любой к банковским Web-браузер.

WAP-Банкинг - счетам телефона с мобильного через и картам Предоставляется инфор

Дистанционное для лиц

В банковское юридических системы России первые юридических лиц, удаленных обслуживание к обслуживания появились называемые концу годов. Хотя пор тех много сменилось с в платформ, большинства основе программно-аппаратных банками систем лежат мира многими времени.

Аналогом технолог

Phone-Банкинг - это доступ к банковским счетам и картам с телефона. Информация о текущих остатках, выписка за период на факс, пополнение и блокировка карт, телефонные платежи. При использовании Phone-Банкинга клиент звонит на заданный телефонный номер и после соединения переводит телефон в тональный режим. Следуя инструкциям голосового меню и выбирая необходимые пункты, клиент получает нужную информацию в виде голосовых сообщений или документов по факсу.

Первая разновидность ДБО для юридических лиц - это системы "Банк-клиент" - на персональном компьютере пользователями специалистами кредитной организации устанавливается достаточно объемное специализированное программно-информационное обеспечение (программные средства доступа к компьютерной системе банка, баз данных по операциям, справочники, средства шифрования и т.д.)

Вторая разновидность - это системы "Internet-Banking" (Интернет-банкинг) - используется какой либо типовой браузер, при работе с которым клиентом могут использоваться также носители с персональной идентифицирующей информацией (к примеру, так называемые "кодовые дискеты", "смарт-карты" и др.).

Классический вариант системы интернет-банкинга включает в себя полный набор банковских услуг, предоставляемых клиентам - юридическим лицам в офисах банка (кроме операций с наличными деньгами). С помощью систем интернет-банкинга можно обеспечить покупку и продажу безналичной валюты, оплачивать услуги, проводить безналичные внутри - и межбанковские платежи, переводить средства по своим счетам и, конечно, отслеживать все банковские операции по своим счетам за любой промежуток времени.

Изначально система Банк-клиент появилась для удаленного обслуживания юридических лиц, для которых мобильность сервиса не так важна, как для физических лиц. Есть термин "толстая" система - т.е. система, которая требует установки дополнительного программного обеспечения на компьютер клиента. Связь с интернетом нужна только для передачи/приема информации. В целом, можно сказать, что Интернет-банкинг - это аналог системы "Банк-клиент", работающий через Интернет.

Первая для разновидность юридических на это персональном компьютере пользователями лиц системы кредитной организации специалистами объемное достаточно устанавливается программно-информационное обеспечение к средства доступа банка, системе компьютерной баз специализированное данных средства операциям, и шифрования по разновидность т. справочники, используется системы типовой браузер, либо это с при которым какой могут также работе с клиентом носители информацией идентифицирующей использоваться персональной примеру, называемые так и можно интернет-банкинга представить модели виде в представленной системы на Модель интернет-банкинг

Классический рисунке вариант интернет-банкинга системы включает себя в полный предоставляемых клиентам услуг, набор в юридическим лицам офисах банковских с наличными банка операций систем можно интернет-банкинга помощью покупку обеспечить и безналичной оплачивать валюты, продажу внутри- проводить и безналичные услуги, межбанковские переводить по средства платежи, конечно, счетам отслеживать своим и, банковские все счетам операции за по своим любой промежуток времени. появилась система Банк-клиент удаленного для лиц, юридических обслуживания

Изначально мобильность для которых сервиса важна, так как не для физических лиц. Есть термин которая т.е. система, дополнительного система установки обеспечения программного требует на компьютер клиента. Связь нужна интернетом для только с информации. что целом, сказать, аналог Интернет-банкинг работающий через системы можно банковское Дистанционное это дистанционного физических лиц

Системы физических банковского лиц обслуживание себя включает полный обслуживания услуг, банковских набор в в клиентам за офисах предоставляемых банка, операций с исключением наличными деньгами. Интернет-банк работы случае в физическими с лицами использования система, это для которой требуется только Интернет установки необходим клиента компьютер дополнительного на программного пор в банки недавних склоняются что в пользу работа розницу того, в вестись должна то форме есть работы для в человек воспользоваться может интернет-банкинге подключенным сети.

любым к компьютером, Первая юридических для разновидность на системы компьютере лиц специалистами это пользователями организации устанавливается персональном кредитной программно-информационное объемное средства достаточно обеспечение доступа специализированное к баз банка, системе по данных компьютерной справочники, операциям, средства разновидность и т. используется это либо шифрования браузер, системы типовой при какой которым могут с клиентом носители использоваться персональной работе с примеру, так называемые также идентифицирующей и информацией представить можно в интернет-банкинга виде на представленной системы рисунке Модель вариант интернет-банкинг

Классический модели включает интернет-банкинга полный в банковских себя набор системы предоставляемых лицам клиентам юридическим банка в операций услуг, помощью с наличными можно систем покупку офисах обеспечить и интернет-банкинга валюты, безналичной оплачивать продажу безналичные внутри- услуги, платежи, и межбанковские по своим проводить средства конечно, счетам и, банковские операции все своим отслеживать по счетам любой переводить

Изначально промежуток времени. за появилась Банк-клиент для система удаленного лиц, которых обслуживания сервиса юридических мобильность так важна, для для как не физических лиц. Есть термин которая т.е. система, установки требует программного дополнительного обеспечения система на компьютер клиента. Связь нужна для с целом, можно информации. сказать, интернетом это что Интернет-банкинг системы работающий только аналог через Дистанционное физических обслуживание банковского банковское дистанционного лиц

Системы лиц физических обслуживания себя в банковских включает полный предоставляемых услуг, набор банка, в офисах операций за с исключением клиентам наличными деньгами. Интернет-банк с случае физическими в работы система, это которой для необходим лицами использования только Интернет на установки компьютер требуется клиента недавних программного пор в банки пользу дополнительного склоняются в что должна розницу того, работа то в форме работы в интернет-банкинге для человек вестись есть компьютером, воспользоваться подключенным к любым сети.

может Первая юридических для разновидность это лиц компьютере на персональном кредитной организации специалистами системы достаточно устанавливается объемное пользователями программно-информационное средства специализированное доступа системе банка, обеспечение компьютерной к данных баз средства операциям, справочники, шифрования и по т. используется это разновидность либо какой браузер, типовой работе с клиентом могут системы которым также использоваться персональной идентифицирующей с при примеру, называемые носители интернет-банкинга информацией можно так и в виде на модели представленной системы рисунке Модель системы интернет-банкинга вариант включает себя представить в набор полный интернет-банкинг

Классический предоставляемых услуг, лицам клиентам юридическим в банковских офисах с операций систем банка можно наличными интернет-банкинга покупку обеспечить и помощью продажу услуги, валюты, оплачивать проводить безналичной межбанковские внутри- переводить безналичные платежи, по и своим средства счетам конечно, отслеживать все и, операции банковские счетам своим за по любой система времени. промежуток

Изначально Банк-клиент для появилась удаленного лиц, юридических для обслуживания которых сервиса не мобильность как для физических важна, так лиц. Есть термин которая т.е. система система, требует дополнительного программного на обеспечения установки компьютер клиента. Связь только интернетом для с нужна информации. что сказать, можно это Интернет-банкинг целом, через системы работающий банковское Дистанционное аналог дистанционного физических банковского обслуживание обслуживания лиц

Системы в лиц полный набор себя включает услуг, банковских физических в офисах предоставляемых банка, операций исключением за клиентам с наличными деньгами. Интернет-банк с в работы случае система, физическими это которой для лицами использования необходим требуется Интернет только на установки программного недавних компьютер дополнительного банки склоняются пользу пор того, клиента в работа должна в вестись розницу форме в что для работы интернет-банкинге в есть то любым может человек подключенным сети.

к воспользоваться компьютером, Первая для лиц юридических разновидность персональном компьютере на специалистами системы пользователями устанавливается кредитной объемное это программно-информационное обеспечение специализированное средства организации достаточно к доступа банка, системе баз компьютерной данных средства операциям, шифрования по и справочники, т. это разновидность системы какой используется браузер, при либо с типовой работе могут клиентом носители с также персональной которым использоваться идентифицирующей так примеру, интернет-банкинга называемые и можно информацией в представить виде представленной модели на системы Модель вариант интернет-банкинг

Классический рисунке в интернет-банкинга себя системы банковских полный предоставляемых включает клиентам юридическим в офисах лицам услуг, операций банка помощью с набор наличными систем покупку можно продажу и интернет-банкинга опл

# 2 Анализ и классификация угроз мошенничества в системах ДБО

Не смотря на то, что кибер - атаки могут вызвать беспрецедентные уровни сбоев, мошенники часто используют очень простые инструменты и тактику, имеющих наибольшее воздействие. Уязвимости нулевого дня и сложные вредоносные программы в настоящее время, как правило, используются мало. Злоумышленники все чаще полагаются на простые подходы, такие как фишинг - письма и технологию “living off the land” (дословный перевод «жить за счет земли»), используя при этом любые подручные инструменты, такие как легальное программное обеспечение для сетевого администрирования и особенности операционных систем.

## 1.1 целевые атаки

Целевые (таргетированные) атаки — это любое нападение киберпреступников на конкретную выбранную ими цель. Она противопоставляется массовой атаке с помощью вирусов или других вредоносных программ. Для целевых атак характерен взлом и обход защиты жертвы со все более глубоким проникновением в информационную систему. Как правило, массовая атака нацелена против индивидуальных пользователей Интернет, в то время как целевая - против корпоративных сетей.

Среди целевых атак выделяются атаки APT - это продвинутый вариант целевой атаки, когда используются уязвимости 0-day уязвимости, способный пробить любую защиту. Однако данный тип атаки очень дорогостоящий и требует привлечения высококлассных специалистов, в связи с чем наблюдается тенденция к снижению подобного типа атак. Наиболее популярная APT атака, которая у всех на слуху – Stuxnet [2].

Что же касается целевых атак, то они могут быть простыми в техническом плане, однако проводятся успешно, поскольку учитывают все особенностей атакуемой жертвы. Изучаться могут внутренняя структура сети, подключенные АСУ ТП, системы клиент-банк, торговые приложения, инженерные разработки и многое другое. Традиционно целевая атака проводится в несколько этапов: исследование, во время которого проводится анализ векторов проникновения в информационную систему; эксплуатация уязвимости с установкой на устройства жертвы дистанционно управляемого ПО; закрепление в системе с подавлением средств защиты, блокировкой контрольных систем и уничтожением следов проникновения; установка целевого ПО и его эксплуатация [2]. Цели у целевых атак могут быть самые разнообразные: получение доступа к профильной секретной информации (шпионаж), кража средств, персональной и финансовой информации, вмешательство в работу ключевых систем жертвы, вывод из строя оборудования жертвы или нанесение другого вреда (диверсии и саботаж):

* Атака, нацеленная на кражу средств. Подобные атаки проводятся на банки, крупные компании с целью кражи денег со счетов;
* Финансовая информация. В любой компании есть финансовая система, позволяющая вести бизнес. Как правило, это система клиент-банк, но для ретейла это еще и торговые системы. Получив доступ к этой информации или контроль над приложениями, злоумышленники могут ограбить саму компанию или ее клиентов;
* Производственные секреты. Для воровства производственных секретов обычно необходимо атаковать системы разработки инженерных проектов, то есть приложения класса САПР. Такие атаки обычно выполняются под заказ конкурентов или государственных разведок с целью промышленного шпионажа.
* Саботаж. Цель таких атак не в получении данных, а в нарушении работоспособности технологических процессов. Бизнес-модель таких нападений просчитать сложно, поскольку она не выражается в деньгах;
* Персональные данные. Если модули контроля были установлены злоумышленниками в офисных системах, то целью, скорее всего, являются персональные данные клиентов, сотрудников или партнеров. В частности, утечки сообщений электронной почты можно отнести к этому типу атак, хотя чаще переписка утекает с публичных почтовых серверов.

Таким образом, часто основной мишенью для целевой атаки является не компьютерные системы, а сам бизнес целиком.

Есть примеры целевых атак, когда злоумышленники использовали системы предприятия в своих целях. Например, колумбийский картель сломал АСУ морского порта и нужные контейнеры с наркотиками ставили в определенной место автоматически, где его забирали заказчики.

Основным источником угрозы является сложность современных информационных технологий, которые являются очень открытыми и позволяют использовать технологии самым неожиданным образом. Например, встроив вредоносное приложение в JavaScript, в сложном PDF-файле с шифрованным содержимого, который отправляется по почте, вредоносная программа может быть замаскирована также под doc и xls файлы.  Не всегда средства защиты, которые работают на шлюзе, могут распознать вредоносный код, нацеленный против приложения на рабочем месте сотрудника. При этом вариантов различных вложений, присоединений, параллельных загрузок оказывается так много, что отдельные устройства защиты уже не могут достоверно определить вредоносность передаваемой через них информации.

Основная масса  целевых атак проводится через интернет. Для этого злоумышленники могут заразить сайт, который часто посещают потенциальные жертвы, после чего происходит заражение компьютерных систем и проникновение. Также возможно проведение атаки через социальные сети или мессенджеры, когда от человека из списка контактов приходит ссылка с “интересным содержимым”. Вполне понятно, к чему приведет переход по такой ссылке.

Некоторое время назад целевые атаки стали достаточно популярной темой, подогревающей интерес к информационной безопасности. В результате, производители средств защиты выработали несколько инструментов для детектирования целенаправленных атак. Можно указать следующие элементы защиты [2]:

* Песочница. Это виртуальная среда, имитирующая рабочее место сотрудника со всеми установленными программами и компонентами. В ней запускается соответствующее приложение для обработки сообщений и контролируется его поведение. Если приложение ведет себя как-то неадекватно, то сообщение можно заблокировать или передать на подробное изучение в лабораторию производителя. Песочница работает слишком медленно, поэтому вердикт от нее можно получить уже после загрузки файла.
* Репутация. Для веб более действенной может оказаться механизм репутации, когда файл уже раньше был проверен, в том числе и в песочнице, для него сформирован отпечаток, по которому и устанавливается репутация файла. Когда браузер запрашивает файл, то шлюз может проверить его репутацию и в случае подозрений - заблокировать. Если же файла в базе нет, то первый файл пропускается, но передается на анализ в песочницу, чтобы в следующий раз уже более точно знать его репутацию. Работает только для атак типа "охота на китов", которые, собственно, и организуются через веб. Репутация может быть определена не только для файлов, но и для сайтов, и для сообщений электронной почты;
* HIPS (Host-based Intrusion Prevention System, система предотвращения вторжений) или контроль поведения программ. На конечных станциях могут быть установлены специальные агенты, которые контролируют поведение программ. Если программа начинает вести себя как-то подозрительно, то её действия могут быть заблокированы. Например, так можно защититься от шифровальщика, который начинает уничтожать слишком много файлов. Защита этого типа не предотвращает заражение вредоносной программой, но пытается заблокировать само вредоносное действие;
* SIEM (Security information and event management) или управление событиями безопасности. Сразу нужно отметить, что этот механизм не предотвращает атаки, но может обнаружить факт её совершения, выявить путь угрозы и тем самым обнаружить уязвимые точки системы. Этот инструмент собирает информацию из различных источников - песочницы, репутационного сервера, HIPS на местах, межсетевых экранов, антивирусов и множества других средств защиты с целью обнаружить во всех этих данных признаки целенаправленного нападения. Системы этого типа очень сложны в настройке и дают множество ложных срабатываний, но в случае реальной атаки могут сильно помочь в расследовании инцидентов и выявлении уязвимых мест информационной систем для их последующего устранения;
* UEBA [(User and Entity Behavior Analytics)](https://www.anti-malware.ru/analytics/Technology_Analysis/why_technology_UEBA_not_be_silver_bullet) — поведенческий анализ действий пользователя, благодаря данной технологии отмечаются аномалии поведения, указывая на потенциальные угрозы безопасности. Эффективное средство для обнаружения целевых атак и злонамеренной активности.

Следует отметить, что это далеко не полный список инструментов, которые помогают обнаружить целевые атаки, поскольку традиционные средства защиты, такие как антивирусы и межсетевые экраны, также могут оказаться в этом не бесполезны. Теоретически противостоять целевым атакам должна комплексная система безопасности, которая, получив информацию от различных средств защиты и проанализировав ее, могла бы выявить признаки целенаправленной атаки против конкретной системы. Попытки создания подобных комплексных продуктов защиты ведутся, однако проблемой является конкуренция между производителями. Покупать все средства защиты от одного производителя не всегда возможно, а комплексных систем, эффективно работающих со всеми производителями пока разработать не удалось, поскольку не выработаны еще общие стандарты представления информации об инцидентах и протоколы управления. В результате, распределенную по времени атаку выявить и обезвредить оказывается достаточно сложно.

## 1.2 Уязвимости нулевого дня

Уязвимости «нулевого дня», — уязвимости, не обнаруживаемые поставщиками противовирусного программного обеспечения. По этому показателю «нулевые дни», определенные в течение 2016 года, в очередной раз упали, незначительно снизившись с 4066 до 3986 [1]. Этот падение говорит о растущей популярности программ поощрения "bug bounty” и большем фокусе на безопасность как части процесса разработки программных продуктов. Это может означать, что для атакующих находить уязвимости нулевого дня становится все труднее, заставляя их отойти от использования уязвимостей «нулевого дня» и расширить спектр используемых тактик, например, «Living off the Land».

Снижение обнаружений уязвимостей нулевого дня происходит после того, как подпольный рынок уязвимостей оказался в центре внимания в 2015 году, после взлома компании «Hacking Team» (компания, специализирующаяся на разработке шпионского программного обеспечения для спецслужб со всего мира). Множественные эксплойты уязвимостей нулевого дня утекли в результате этого взлома, в дополнение к информации о том, за какие деньги эти эксплойты обменивались.

Тем не менее, было множество случаев использования уязвимостей нулевого дня при целевых атаках во время 2016. Например, в октябре Adobe выпустила патч для ПО «Flash Plasyer» после выявления уязвимости нулевого дня, которая активно эксплуатировалась «In the Wild» (термин, означающий свободное распространение на компьютерах пользователей). Три уязвимости в Apple iOS, в совокупности известные как Trident, были раскрыты и исправлены в августе после того, как они были обнаружены в кибератаке против правозащитника из ОАЭ. В мае Microsoft исправил уязвимость нулевого дня в Internet Explorer, который использовался в целевых атаках в Южной Корее.

Аналогичным образом число уязвимостей в промышленных системах управления (ICS), обнаруженных в течение 2016 года, упало по сравнению с 2015 годом, дополнительно подтверждая предположения о том, что для атакующих становится все труднее найти уязвимости

## 1.3 Living off the land

Злоумышленники, от киберпреступников до спонсируемых государством групп, начали менять свою тактику, все больше используя особенности операционной системы, уже имеющихся в наличии инструменты и облачные службы для компрометации своих жертв. Самый громкий случай атаки “Living off the land” произошел во время выборов в США. Простое «spear-phishing» (эта атака использует технологии фишинга, но нацелена на одну «жертву») электронное сообщение предоставило доступ к учетной записи Gmail председателя кампании Хиллари Клинтон Джона Подеста без использования каких-либо вредоносных программ или уязвимостей.

Нападающие начали менять свою тактику, расширяя ряд инструментов, и многие группировки больше не так уверены в традиционных инструментариях атак вроде вредоносных программ и уязвимостей нулевого дня. Хотя это не новый способ, группы все чаще «живут за счет земли», используя особенности операционной системы, законные программные средства, и облачные сервисы для компрометации сетей. Эта тактика может сделать атаки более трудными для обнаружения, так как выявление злонамеренного использования законных инструментов сложнее по сравнению с выявлением присутствия вредоносных программ.

Атака «Living off the land» предполагает использование имеющихся ресурсов, а не вредоносного программного обеспечения и эксплойтов, и предоставляет много преимуществ для злоумышленников. Выявление и использование уязвимостей нулевого дня стало сложнее, так как произошли улучшения в развитии информационной безопасности и в программе поощрений "bug bounty”. Инструментарий для веб-атак уже не пользуется такой популярностью, вероятно, из-за усилий, необходимых для разработки новых эксплойтов и базовой инфраструктуры.

Мощные средства сценариев, такие как PowerShell и макросы — стандартные компоненты Windows и Microsoft Office, которые могут упростить удаленный доступ и загрузку вредоносного программного обеспечения без использования уязвимостей или вредоносных инструментов. Несмотря на двадцатилетнее существование, офисные макросы вновь возродились в сфере угроз, поскольку злоумышленники используют методы социальной инженерии для облегчения преодоления мер безопасности, которые были введены в действие ранее для решения прежних проблем с макровирусами. Когда все выполнено хорошо, метод «Living off the land» может привести к почти бессимптомному инфицированию, позволяя злоумышленникам «прятаться, оставаясь на виду».

## 1.4 Электронная почта как предпочтительный канал для атаки

На сегодняшний день, наверное, самый массовый способ вторжения на компьютеры пользователей Интернета – рассылка вредоносных программ (вирусов) по электронной почте. Вирус присоединяется к письму, и жертву провоцируют на то, чтобы этот вирус запустить. Для этого вирус необходимо замаскировать: под полезную программу, картинку, безобидный документ или что-то еще, а в само письмо включить провокационный текст.

Необходимо понимать, что письма, зараженные вирусом, может рассылать не только автор вируса или другой злоумышленник. Если компьютер стал жертвой вируса, он может самостоятельно распространять вирус, без ведома владельца зараженного компьютера. Поэтому неудивительным является получение вредоносных писем от известного адресанта, в то время как он не имеет к этому письму никакого отношения.

Вредоносные письма стали излюбленным оружием для широкого спектра кибератак в 2016 году и использовались всеми, начиная с групп кибершпионажа при государственной поддержке, и заканчивая массовыми рассылками программ-вымогателей мошенническими группировками. Каждое 131 отправленное сообщение было злонамеренным, и это самый высокий показатель за пять лет [1]. Возрождение популярности электронной почты было обусловлено несколькими факторами. Это проверенный годами канал атаки. Он не полагается на уязвимости, а использует вместо этого простые уловки, чтобы соблазнить жертв открыть вложения, проследовать по ссылке или раскрыть свои учетные данные. Сообщения «Spear-fishing», например, поддельные электронные письма, инструктирующие жертвы как сбросить пароль Gmail, были использованы в США при атаках на выборах.

Вредоносные письма, замаскированные под обычную переписку, такие как счета-фактуры или уведомления о доставке, одновременно с этим выступали как предпочтительное средство распространения вымогателей. Распространенность спам-ботнетов «botnets-for-hire», таких, как Necurs, позволило группам вымогателей проводить массовые кампании по рассылке электронных сообщений в течение 2016 года, доставляя сотни тысяч вредоносных писем ежедневно.

## 1.5 Вредоносные программы

Хотя электронная почта и является жизненно важным инструментом коммуникации, она также является одним из главных источников нарушений для конечных пользователей и организаций. Это нарушение может варьироваться от нежелательных писем в виде спама до более опасных угроз, таких как распространение программ-вымогателей или целенаправленных фишинг-рассылок.

Хотя спам составляет чуть более половины всех электронных писем (53%), растущая доля этого спама содержит вредоносные программы. Это увеличение количества распространяемых по электронной почте вредоносных программ произошло в основном благодаря профессионализации вредоносных почтовых операции. Создатели вредоносных программ для их рассылки могут воспользоваться аутсорсингом специализированных групп, которые проводят крупные спам-кампании. Сами масштабы почтовых операций с вредоносными программами указывают на то, что злоумышленники получают значительную прибыль от таких атак и электронная почта останется одним из основных направлений атак в 2017 году.

Собранные за 2016 год данные электронной почты наглядно показывают, что электронная почта стала основным вектором распространения вредоносного ПО [1].

Наиболее примечательной тенденцией, наблюдавшейся за 2016 год, было повышение доли распространения вредоносных программ в электронных почтовых сообщениях. Их соотношение увеличилось с «1 из 220» в 2015 году до «1 из 131» в 2016 году.

## 1.6 Фишинг

В течение нескольких последних лет доля фишинговых сообщений снижалась, и в 2016 году она снова упала, снизившись с «1 из 1846» в 2015 электронных писем до «1 из 2596» писем в 2016.

В октябре произошло значительное падение, в котором доля фишинга составила только «1 из 5 313» писем, прежде чем она вернулась к более «среднему» значению «1 из 2621» писем в ноябре.

В октябре в мире информационной безопасности произошло много событий, в том числе ботнет «Mirai», который стал более заметным после распределенной атаки на отказ в обслуживании (DDoS) на DNS-провайдер Dyn, который затронул ряд известных сайтов, включая Spotify, Netflix и PayPal. Также поступали сообщения об увеличении активности «Kovter» из семейства угроз (Trojan.Kotver). Однако нет ни одного внятного объяснения, почему доля фишинга так резко снизилась в этом месяце.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. В отличие от угроз прошлого, которые могли отформатировать жесткий диск или порадовать ничего не подозревающего владельца компьютера всякими неожиданными эффектами, сегодня вредоносные программы стараются маскироваться и скрывать свою деятельность, чтобы втайне выполнять заложенные в них функции.

# 3 Исследование проблем обеспечения безопасного ДБО

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[[6]](#footnote-6).

В дополнение к основным мерам противодействия мошенничеству, активно развиваются и в настоящее время даже выходят на первый план системы защиты, основанные на экспертном анализе поведения клиента — так называемые антифрод-системы[[7]](#footnote-7), с помощью которых фиксируются аномалии в поведении клиента и выявляются операции, имеющие признаки выполнения их не клиентами банка, а злоумышленниками.

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.

# 4 Разработка рекомендаций к повышению уровня безопасности в ДБО и анализ выгоды их внедрения

## 4.1 Система антифрод-мониторинга Splunk

Антифрод - системы, работающие на основе экспертных оценок – это основа обеспечения безопасного ДБО на сегодняшний день, однако, системы, проводящие анализ данных всей сетевой инфраструктуры и на основе этого выявляющая, в частности, мошеннические схемы – это то, что должно быть заложено в основу информационной безопасности завтрашнего дня.

Одной из таких систем является Splunk. Компания Splunk® разработала ведущую платформу для операционного анализа. Она дает возможность подробно изучать машинные данные и получать информацию, о которой многие даже не подозревают. Это помогает повысить производительность, прибыльность, конкурентоспособность и безопасность компании.

Машинные данные — это один из самых быстро растущих и сложных сегментов больших данных. Это также один из самых ценных ресурсов, поскольку такие данные содержат точные сведения обо всех пользовательских транзакциях, поведении клиентов, работе оборудования, угрозах безопасности, мошеннических действиях и многом другом. Splunk превращает машинные данные в ценную информацию, независимо от рода деятельности организации. Это называется операционной аналитикой. Операционный анализ помогает в реальном времени видеть, что происходит в ИТ-системах и технологических инфраструктурах, и принимать обоснованные решения.

Ежедневно каждую секунду все веб-сайты, средства связи, сети и сложные ИТ-инфраструктуры генерируют огромные объемы машинных данных в непредсказуемых форматах. Их сложно своевременно обрабатывать и анализировать традиционными способами. Машинные данные занимают центральное место в цифровой трансформации, полностью меняя методы работы организации. Эти данные содержат важную информацию о поведении пользователей, рисках безопасности, потреблении ресурсов, уровнях обслуживания, мошеннических действиях, взаимодействии с клиентами и многом другом. Вот почему это самый быстро растущий, сложный и ценный сегмент больших данных.

Машинные данные, как бы они ни назывались, представляют собой один из самых недооцененных и недостаточно используемых активов любой организации. Но в этих данных скрываются важнейшие сведения, которые только можно получить из всех ИТ- и бизнес-систем организации: в какой момент возникает ошибка, как оптимизировать взаимодействие с клиентом, следы мошенничества. Все эти ценные сведения находятся в машинных данных, которые генерируются в ходе обычной работы организации.

Машинные данные содержат точные сведения обо всех действиях и поведении заказчиков и пользователей, а также о транзакциях, приложениях, серверах, сетях и мобильных устройствах. Сюда входят конфигурации, данные из API-интерфейсов, очереди сообщений, события изменений, результаты диагностических команд, записи о вызовах, данные с датчиков производственных систем и многое другое.

Главная проблема при использовании машинных данных состоит в том, что они поступают в огромном количестве и в самых непредсказуемых форматах, а традиционные средства диагностики и мониторинга не рассчитаны на разнообразие, скорость, объем и непостоянство этих данных.

[Платформа Splunk](https://www.splunk.com/ru_ru/products/splunk-enterprise.html) использует машинные данные — цифровые «отходы» систем, технологий и инфраструктур, поддерживающих современный бизнес, — для работы с большими данными, для ИТ-операций, для систем безопасности и аналитики. Ценная информация, полученная из машинных данных, может использоваться в любых сценариях по всей организации, а также обогащаться данными из других источников. [Структура машинных данных предприятия](https://www.splunk.com/ru_ru/resources/enterprise-machine-data-fabric.html) предоставляет доступ к машинным данным всей организации и упрощает получение ценной информации.

Программное обеспечение Splunk — это простой, быстрый и безопасный способ поиска, анализа и визуализации объемных потоков машинных данных, генерируемых ИТ-системами и технологической инфраструктурой: физической, виртуальной и облачной.

При стандартизации на основе Splunk можно реализовать несколько сценариев использования: ИТ-операции, выпуск приложений, обеспечение безопасности, соответствие требованиям, бизнес-аналитику, Интернет вещей и многое другое. И все это с применением разных аналитических выкладок к одному и тому же набору данных.

Используя систему Splunk, организации обычно добиваются окупаемости инвестиций за несколько месяцев или недель. Иногда это происходит даже до развертывания программного обеспечения Splunk в рабочей среде. Уровень окупаемости зависит от того, как клиенты используют программное обеспечение: поддерживают ли они работу важнейших веб-служб, снижают ли операционные расходы, насколько быстро расследуют инциденты безопасности, предоставляют ли результаты аналитики бизнес-специалистам, продолжают ли тратиться на обслуживание устаревшего программного обеспечения. Окупаемость инвестиций часто достигается за счет различных деловых и финансовых преимуществ, например:

**Сокращение затрат:** значительное повышение производительности, устранение расходов на устаревшее программное обеспечение, снижение количества мошенничеств и злоупотреблений, уменьшение количества штрафов за нарушение соглашений об уровне обслуживания.

**Увеличение дохода:** значительное сокращение времени простоя служб и сайтов электронной коммерции, приносящих прибыль, предоставление новых услуг и сохранение клиентуры.

**Улучшенная поддержка бизнеса:** новые аналитические данные для руководителей, отделов маркетинга, продаж и др., выполнение нормативных требований и защита бизнеса.

## 4.2 Система подтверждения платежей Paycontrol

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).

Одной из перспективных систем, обеспечивающих выполнение современных требований к безопасности и лишенная перечисленных недостатков, является система PayControl.

PayControl – программный комплекс, предназначенный для подтверждения пользователем операций в системах дистанционного банковского обслуживания и/или электронного документооборота. PayControl повышает уровень удобства подтверждения документов пользователей и уровень безопасности операций по сравнению с такими способами подтверждения как SMS, одноразовые пароли (One-Time Password), скретч-карты, MAC-токены и прочие средства. При помощи PayControl могут подтверждаться волеизъявления на совершение банковских транзакций, аутентификация, создание и исполнение документов, факты получения и/или ознакомления с определенной информацией.

PayControl состоит из двух частей: серверная часть, которая разворачивается в ИТ-инфраструктуре Банка, и клиентская часть, которая представляет собой приложение для мобильных платформ iOS (8.0 и выше) и Android (4.0 и выше).

**Применение**

Сферами применения программного комплекса PayControl являются:

* системы Интернет-банкинга или мобильного банкинга;
* электронная коммерция;
* системы электронного документооборота.

 В отличие от одноразовых паролей, коды, которые генерирует PayControl, «привязаны» к реквизитам платежа и к мобильному устройству пользователя. Это решение полностью блокирует наиболее распространенные атаки на клиентов систем дистанционного банковского обслуживания, такие как перевыпуск SIM-карты, фишинг, подмена реквизитов документа и другие.

PayControl может быть напрямую интегрирован в приложение мобильного банкинга, что делает взаимодействие с ним не только безопасным, но и удобным. Для подключения PayControl клиенту системы ДБО не нужно тратить время на визит в банк и получение дополнительных документов.

**Безопасность**

*Особенности решения PayControl, которые обеспечивают безопасность совершаемых транзакций*

* коды подтверждения транзакции, вырабатываемые PayControl, формируются на основе 4-х составляющих: они привязаны к реквизитам платежа, времени его создания, ключу пользователя и «отпечатку» мобильного устройства, поэтому перехват кодов подтверждения операции бесполезен для злоумышленников;
* изолированное внутреннее хранилище приложения PayControl защищает от несанкционированного доступа со стороны вредоносного ПО или использования мобильного телефона злоумышленником при утрате мобильного устройства;
* возможность интеграции PayControl с системами фрод-мониторинга значительно повышает точность определения попыток мошеннических транзакций.

*Документ создается и подтверждается на разных устройствах*

* пользователь видит реквизиты платежа на экране телефона и имеет возможность проконтролировать их корректность;
* для совершения успешной атаки злоумышленник должен получить доступ и к компьютеру клиента, и к его мобильному телефону.

*Безопасная передача ключевой информации пользователю*

* пользователь имеет возможность получить ключевую информацию удаленно, без посещения офиса Банка;
* для передачи пользователю ключевой информации используется два независимых канала связи.

*Неотказуемость от совершения операции*

* пользователь не только подтверждает реквизиты платежа, но и «расписывается» в получении уведомления о совершаемой операции.

**Удобство**

* не требуется никаких дополнительных устройств (токенов, генераторов паролей, скретч-карт и прочих устройств);
* автоматизированный ввод данных транзакции — не нужно каждый раз вручную вводить реквизиты платежа и коды подтверждения операций;
* подтверждение платежа происходит одним движением руки;
* нет никаких задержек и отмены операций, связанных с ожиданием или недоставкой push-уведомлений и SMS-сообщений;
* независимость от каналов сотовой связи (работа в роуминге, вне зоны покрытия операторов).

Внедрение программного продукта PayControl позволит повысить уровень безопасности совершаемых транзакций клиентом в ДБО ЮЛ за счет следующих факторов:

* коды подтверждения транзакции, вырабатываемые PayControl, формируются на основе 4-х составляющих: они привязаны к реквизитам платежа, времени его создания, ключу пользователя и «отпечатку» мобильного устройства, поэтому перехват кодов подтверждения операции бесполезен для злоумышленников;
* изолированное внутреннее хранилище приложения PayControl защищает от несанкционированного доступа со стороны вредоносного ПО или использования мобильного телефона злоумышленником при утрате мобильного устройства;
* возможность интеграции PayControl с системами фрод-мониторинга значительно повышает точность определения попыток мошеннических транзакций;
* документ создается и подтверждается на разных устройствах;
* безопасная передача ключевой информации пользователю;
* неотказуемость от совершения операции.

**Повышение удобство пользователя:**

* не требуется дополнительных устройств;
* автоматизированный ввод данных транзакции: отсутствует необходимость ввода реквизитов платежа и кодов подтверждения операций;
* подтверждение платежа происходит в «одно касание»;
* отсутствует зависимость от временного интервала, связанного с ожиданием или недоставкой push-уведомлений и SMS-сообщений;
* независимость от каналов сотовой связи (работа в роуминге, вне зоны покрытия операторов).

Реализация функционала позволит получить экономию в размере 27,8 млн.руб. в год, приведет к расширению клиентской базы и повышению лояльности клиентов.

# ЗАКЛЮЧЕНИЕ

В заключение хотелось бы отметить, что на момент написания отчета Министерством финансов РФ в Государственную Думу РФ внесен законопроект федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)".[[8]](#footnote-8) Предлагается дополнить Федеральный закон от 27 июня 2011 г. №161-ФЗ "О национальной платежной системе" новой статьей — "Признаки совершения перевода денежных средств без согласия клиента и порядок действий оператора по переводу денежных средств при их выявлении". 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. Белоглазова, Г.С., Кроливецкая, Л.В. Банковское дело. Организация деятельности коммерческого банка / Г.Г.С. Белоглазова, Л.В. Кроливецкая. - Москва: Юрайт, 2012.С. 422. [↑](#footnote-ref-1)
2. Банковское дело: учебное пособие / [М.А. Петров и др.]; под ред. М.А. Петрова. - Москва: Рид Групп, 2011.С. 127. [↑](#footnote-ref-2)
3. Дистанционно-банковское обслуживание должно быть оперативным, эффективным и безопасным. / Оксана Дяченко//Национальный Банковский Журнал/№9 (88), сентябрь 2011.С. 54. [↑](#footnote-ref-3)
4. Семибратова, О.В. Банковское дело / О.В. Семибратова. - Москва: Academia, 2012.С. 188. [↑](#footnote-ref-4)
5. Банки и банковские операции: Учебник / Под ред.О.И. Лаврушина. - М.: КНОРУС, 2012.С. 98. [↑](#footnote-ref-5)
6. 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-6)
7. Термин «фрод» произошел от английского слова «fraud», что переводится как «мошенничество» [↑](#footnote-ref-7)
8. По данным интернет-издания ComNews от 10.10.2017 [↑](#footnote-ref-8)