ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**
**( Н И У « Б е л Г У » )**

ИНСТИТУТ ЭКОНОМИКИ
КАФЕДРА ФИНАНСОВ, ИНВЕСТИЦИЙ И ИННОВАЦИЙ

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Выпускная квалификационная работа
обучающегося по направлению подготовки 38.03.01 Экономика
заочной формы обучения, группы 06001351
Чернобровой Виктории Романовны

Научный руководитель
д. э. н., профессор кафедры
финансов, инвестиций и инноваций
Флигинских Т.Н.

БЕЛГОРОД 2018

ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

**Актуальность** определяется тем, что банки являются краеугольным камнем кредитно-финансовой системы государства и важнейшим финансовым институтом современного общества. В связи с этим на них возлагаются особые требования к обеспечению информационной безопасности. Дистанционное банковское обслуживание (ДБО) - неотъемлемая часть банковских услуг клиенту с использованием телефонных и компьютерных сетей, без его непосредственного визита в банк. Это инструмент снижения операционных расходов, повышения эффективности и конкурентоспособности бизнеса банков. В исследовании агентства CNews Analytics, проведенном в 2017 году, отмечается стабильный рост уровня распространенности ДБО: такие системы используют 94% российских банков. Согласно данным Банка России доступом к своим банковским счетам пользуется несколько миллионов физических лиц. Распространение ДБО особенно активно происходило в периоды кризисов, на ряду со стремлением руководителей банков сократить свои издержки путем внедрения сравнительно доступной формы обслуживания. Вместе с тем недостаточное внимание, уделяемое проблемам информационной безопасности и защиты информации, привело к целому ряду уязвимостей, хорошо известных в сфере безопасности приложений, а также угрозам, связанным со спецификой банковской сферы, реализация которых может привести к существенным финансовым и репутационным потерям.

Возрастание роли информационной безопасности дистанционного банковского обслуживания вызывает необходимость исследования современной практики организации и выявления негативных тенденций в целях их предотвращения.

Среди отечественных и зарубежных учёных значительный вклад в исследование научных положений теории и практики дистанционного

банковского обслуживания и его информационной безопасности внесли: А.Г.Братко, Ван Хорн Дж.К, В.С.Волынский, Э.Долан, Е.Ф.Жуков, А.А.Казимагомедов, О.И.Лаврушин, В.Лексис, Г.Х. Азнобаева, В.В.Масленников, В.Д.Миловидов, Л.Миллер, Г.С.Панова, Э.Рид, Ж.Ривуар, А.Х. Айтуганова, Е.С. Переверзева, Е. В. Илинич, Г.А.Тосунян, В.А.Челноков, В.М.Усоскин, Д.В. Фурманов и др.

**Цель** выпускной квалификационной работы состоит в изучении теоретических основ информационной безопасности дистанционного банковского обслуживания и разработке комплекса мер по ее обеспечению.

Для достижения поставленной цели в работе решались следующие **задачи:**

- дополнение признаков классификации информационной безопасности ДБО;

- рассмотрены традиционные подходы информационной безопасности ДБО;

- выявление факторы, влияющие на информационную безопасность;

- проанализировать условия становления системы информационной безопасности в ПАО Сбербанк;

- обоснованы перспективы выявления и борьбы с различными видами кибератак в целях обеспечения информационной безопасности.

**Объектом** исследования выступает процесс обеспечения информационной безопасности дистанционного банковского обслуживания.

**Предметом** исследования являются организационно-финансовые отношения, связанные с информационной безопасностью дистанционного банковского обслуживания.

**Методологической и теоретической основой исследования** послужили труды зарубежных и отечественных экономистов-финансистов, исследования современных отечественных и зарубежных ученых по

проблемам информационной безопасности, а также проблемы развития дистанционного банковского обслуживания.

В работе используются следующие методы: индукции, дедукции; статистические, аналитические, группировок, монографический; эволюционный, экстраполяции, экспертных оценок, рейтингования, балансовый, коэффициентный, расчетно-конструктивный, экспертный, нормативно-ресурсный.

**Информационную базу** работы составляют законодательные акты Российской Федерации, нормативные документы и статистические материалы Банка России, данные Федеральной службы государственной статистики, материалы научный публикаций, в том числе в сети Интернет, а также бухгалтерская и годовая отчетность банка ПАО Сбербанк за 2016-2017 годы.

**Научная новизна и практическая значимость** заключается в том, что в работе достаточно основательно проанализированы теория и практика информационной безопасности дистанционного банковского обслуживания в коммерческом банке в условиях экономической нестабильности, а также направления повышения эффективности комплекса мер по формированию системы в ПАО Сбербанком, которые могут быть использованы в дальнейших исследованиях и применены банками конкурентами в своей деятельности.

**Структура** выпускной квалификационной работы состоит из введения, двух глав, заключения, списка литературы, приложений.

# ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

## 1.1.Экономическая сущность и виды информационной безопасности

Системы дистанционного банковского обслуживания (ДБО) как инструмент снижения операционных расходов, повышения эффективности и конкурентоспособности бизнеса банков получают все более широкое распространение в нашей стране.

Вместе с тем специалисты по информационной безопасности (ИБ) отмечают низкий уровень защищенности ДБО и большое количество уязвимостей в программном обеспечении, используемом в ДБО-системах, несмотря на увеличение доли профессиональных разработок против самописных.

Проблема уничтожения банковской информации может быть вызвана, как поломкой или сбоями программного обеспечения, так и, например, специальными вирусами, вызывающими сбои операционных систем. Сводят к минимуму потери информации из-за этих факторов ежедневное резервное копирование информации, постоянное обновление операционных систем и специальные защитные программы.

Проблема искажения банковской информации практически всегда связана с человеческим фактором, причем — с собственными человеческими ресурсами банка. Сами сотрудники банка могут сделать ошибку при копировании или транспортировании информации, причем, ошибка может быть, как намеренной, так и автоматической. Решает эту проблему тщательный отбор персонала, имеющего доступ к важной информации,

автоматизация процессов внесения данных, шифрование информации, а также контроль действий рядовых сотрудников со стороны менеджеров.

А вот получение банковской информации третьими лицами — это основная угроза банковской системе, которая может привести к огромным финансовым потерям. На сегодняшний день могут быть применены 3 основных способа несанкционированного доступа к информации:

1. Доступ к местам обработки и хранения информации. Может произойти, как примитивным путем физического взлома офиса банка, взлома электронных источников хранения информации (достаточно редкий случай, учитывая степени защиты таких источников) и кража информации при помощи электронных носителей самими сотрудниками банка.

2. Использование резервных копий. Доступ к копиям информационных блоков менее строг, чем доступ к самим носителям, которые в случае злого умысла или ошибки могут попасть в руки мошенников. В мировой практике было множество случаев кражи денежных средств именно при помощи резервных копий информационных блоков.

3. Несанкционированный доступ со стороны сотрудников банка. Это наиболее вероятный и наиболее частый способ потери информации.

Защита банковской информации от утечки и разглашения третьим лицам производится при помощи следующих инструментов:

- Надежное специализированное программное обеспечение.
- Программы защиты от атаки вирусов и других вредоносных программ извне — антивирусные программы.
- Тщательный отбор и текущий контроль персонала, имеющего доступ к информации; различие в уровнях доступа.
- Системы распознавания пользователей.
- Программы специального шифрования информации.
- Применение межсетевых экранов.
- Защита от физического грабежа.

Несмотря на возросший уровень информационных технологий, позволяющих несанкционированно получить доступ к секретной информации, современный рынок способен предложить эффективные и надежные способы защиты банковской информации, которые совершенствуются с не меньшей скоростью, чем инструменты взлома. Обеспечение информационной безопасности — это одна из наиболее актуальных проблем для каждого банка, в которое вкладывается достаточно большое количество ресурсов.

Таблица 1.1

Основные подходы к определению информационной безопасности

| № п\п | Наимнование | Определение |
|---|---|---|
| 1 | Нормативный | Нормативный подход появился в 80-е годы XX века. Название подхода происходит от слова «норма», означающего некий эталон. Существуют различные стандарты информационной безопасности, документы в которых определены признаки, свойства и требования к безопасным информационным системам, также определена шкала, с помощью которой все системы можно оценить на предмет безопасности. |
| 2 | Теоретический | Теоретический подход основан на построении модели безопасности – некоего абстрактного представления реальной системы с точки зрения безопасности. Полученные модели должны быть теоретически и математически обоснованы. Чем сильнее математическая и теоретическая база построенной модели, тем безопаснее система. |
| 3 | Практический (экспериментальный) | Зарождение практического подхода определения безопасности можно связывать с началом эпохи Интернета. Безопасность системы при этом проверяется на практике: одна система более безопасна, чем другая, если она более устойчива к внешним воздействиям и лучше противостоит угрозам. |

В исследовании агентства CNews Analytics, проведенном в прошлом году, отмечается стабильный рост уровня распространенности ДБО: такие системы используют 94% российских банков из ведущей сотни для обслуживания юридических лиц и 83% — для обслуживания физических лиц. Согласно данным Банка России доступом к своим банковским счетам пользуется несколько миллионов физических лиц.

МВД России сообщает, что растут как количество, так и размеры хищений денежных средств индивидуальных и корпоративных вкладчиков, осуществляемых с использованием ДБО. При этом денег у юридических лиц крадётся в тысячи раз больше, чем у физических.

Ситуация, складывающаяся вокруг ДБО, не оставляет сегодня равнодушными никого из его участников и организаторов — ни клиентов, ни банки, ни правоохранительные органы, ни регуляторов, ни специалистов по ИБ.

В данном обзоре мы постарались рассмотреть специфику организации защиты ДБО, возникающие при этом проблемы и возможные пути их решения с учетом необходимости выполнять нормативные требования к обеспечению безопасности банковских транзакций.

В организации защиты системы ДБО рекомендуют исходить, прежде всего, из экономической целесообразности, т. е. чтобы защита не была дороже защищаемых ресурсов. Хотя есть и более радикальные мнения - полагает, что критерий защищенности ДБО может быть только один: злоумышленник не должен найти способа совершить хищение денежных средств. Джабраил Матиев, руководитель группы информационной безопасности компании IBS Platformix, также настаивает на том, что необходимо не дать злоумышленнику возможность получить управление чужим банковским счетом, при этом неважно, каким образом это достигается.

Таблица 1.2

Классификационные признаки дистанционного банковского обслуживания

| Признак классификации | Виды систем дистанционного банковского обслуживания | | | |
|---|---|---|---|---|
| Вид оказываемых услуг | Информационные | Транксационные | Коммуникационные\ консультационные | |
| Среда обмена данными\ канал доставки | Телефон | Интернет | Сотовая связь | |
| Тип инфармиционной системы | Клиент-банк или PC-банкинг | Интернет-банк | Мобильный банк | |
| Требования к специальному программному обеспечению, устанавливаемому клиентом | «Толстый клиент» | «Тонкий клиент» | | |
| Требования к каналу | Сеансовое соединение | Постоянное соединение (on-line) | | |
| Тип субъекта гражданских правоотношений | Юридическое лицо (business-banking) | ПБОЮЛ | Физическое лицо (concumer-banking) | |
| Способ передачи данных | Цифровой | Голосовой | Почтовый | |
| Степень универсальности предоставяемых операций | Минимальная | Типовая | Комплексная | |
| Наличие получения дополнительной «небанковской» информации | Начисления за коммунальные услуги, билинговые системы | Начисленные налоги | Штраф ГИБДД | |
| Стоимость услуг ДБО | Бесплатно | Платно | | |
| Способ взимания тарифа | Абоненская плата | За оказания услуги\ за транзакцию | Комбинированная оплата | |
| Способ аунтефикации | Логин (пароль) | Электронно-цифровая подпись | Биометрия | |
| Наличие дополнительной (к основной | Таблицы с одноразовыми паролями, скреч- | SSM-сообщения с кодом подтверждения | OTP-токены | Виртуальная (OPT-токены для |

| | | | | |
|---|---|---|---|---|
| электронной подписи) аунтификации клиента | карт | | | смартфонов) |
| Вид носителя для электронной подписи | Файловый носитель | Смарт-карта | Сим-карта | |
| Сособ доступа | Без ограничений | Только со строго оборудованного оборудования, имеющего фиксированные параметры (IP, MAC,IMEA) | | |
| Наличие системы шифрования | Отсутствует | Есть | Есть (ГОСТ) | |
| Наличие системы «антифрод» у банка | Есть | Нет | | |
| Лимиты на операции | Без ограничений | Ограничения на все вид операций | Ограничения на высокорискованные операции | |
| Вид разработчика программного обеспечения | Собственная разработка банка | Стронний разработчик | | |
| Способ владения системой ДБО | Собственность банка | Аутсоссинговая система ДБО | | |

Эксперты обращают внимание на то, что средства защиты ДБО не должны доставлять больших неудобств пользователям системы, в первую очередь ее клиентам. В противном случае они просто будут пренебрегать защитой и применять ДБО с нарушением требований к ИБ.

В организации ИБ систем ДБО рекомендует руководствоваться базовыми критериями защищенности информации: обеспечением конфиденциальности, целостности и аутентичности. При этом целостность информации следует рассматривать не только в отношении платежных поручений, но и применительно к операциям проведения платежа. Аутентичность платежного поручения должна рассматриваться для каждой операции с учетом того, в каком отношении к документу состоит пользователь сервиса ДБО [7, стр.71].

Готовым к практическому использованию руководством по обеспечению ИБ в системах ДБО выглядит перечень ключевых критериев защищённости:

- удобный, интуитивно понятный пользовательский интерфейс;
- доступное и внятное руководство пользователя;
- наличие способов идентификации, альтернативных логин-парольной;
- возможность использования средств аутентификации по выбору клиента (с учётом ограничений, устанавливаемых банком);
- возможность выбора правил и средств доступа к системе;
- промышленная (не “самописная”) система ДБО;
- наличие у системы сертификатов регуляторов.

Из основных характеристик защиты ДБО особое внимание обращается на универсальность мер и средств защиты вне зависимости от методов атак, на возможность адаптации системы защиты в соответствии с изменениями технологий ДБО и бизнес-процессов кредитной организации, а также на способность предотвращать нарушения ИБ автоматически.

## 1.2. Традиционные подходы к защите информации дистанционного банковского обслуживания

Защита клиентов дистанционного банковского обслуживания (ДБО) всегда была проблемой нетривиальной и потому интересной для профильных специалистов. И дело здесь не в защите систем ДБО банка, которая ничем не отличается от обеспечения безопасности любого дистанционного доступа из недоверенной среды, имеет на вооружении целый ряд «лучших практик» и иногда даже попадает под действие регламентирующих стандартов, таких как СТО БР и PCI DSS. Нетривиальным остается одно – защита самих клиентских мест ДБО. Компьютеры клиентов – это внешняя по отношению к

системам банка территория, она не контролируется ИТ- и ИБ-службами банка. Организационные меры здесь в большинстве случаев не действуют – клиент всегда прав. Можно рекомендовать клиенту поставить на рабочее место, к примеру, антивирусное программное обеспечение, но реально работающих рычагов воздействия, гарантирующих выполнение этих рекомендаций, нет. Клиентские места при этом – самая массовая часть системы ДБО. Несмотря на то, что основной ущерб в случае нарушения ИБ на клиентском месте несёт именно пользователь системы, банкам тоже достаётся их «порция» – пока это только репутационные риски, миграция клиентской базы, участие в длительных расследованиях и разбирательствах.

Компьютеры клиентов – это внешняя по отношению к системам банка территория, она не контролируется ИТ- и ИБ-службами банка. При этом, число атак на клиентские места в последнее время всё возрастает. В этой сфере традиционно лидируют составители вредоносного ПО как способные на самую массовую атаку. В России один из наиболее частых видов киберпреступлений – это атаки именно на пользователей систем «Клиент–Банк». И при получении злоумышленниками того или иного вида доступа к счетам юридического лица ущерб в среднем составлял 3–5 млн. рублей на организацию [10, стр.812].

Наиболее распространённые способы атак на системы ДБО: вредоносное ПО (трояны, клиенты бот-сетей и т.д.); фишинг; использование атак типа Man-in-the-Middle для проведения подложных транзакций; внутренние атаки (для корпоративных клиентов); направленные атаки на клиентские места (опять же имеют смысл для корпоративных клиентов). Соответственно, наиболее распространённые векторы атак на системы ДБО – это: хищение ключевой и/или аутентификационной информации с последующим ее использованием либо на месте, либо на удалённом компьютере; проведение транзакций непосредственно с компьютера клиента; подмена легитимных транзакций подложными.

С точки зрения возможностей защиты клиентские места ДБО можно разделить на два вида в зависимости от специфики их применения.

Первый – это защита традиционных решений «Клиент–Банк» (или «Банк–Клиент»), подразумевающих наличие «толстого» клиента и традиционно используемых при работе с юридическими лицами. Этот вариант предусматривает необходимость установки на рабочее место пользователя соответствующего пакета ПО.

Второй – это защита интернет-банкинга. В данном случае в качестве рабочего места пользователя выступает «тонкий» клиент, подразумевающий отсутствие какого-либо специализированного ПО на стороне клиента банка. Этот вариант используется прежде всего при работе с физическими лицами, но приобретает всё большую популярность благодаря отсутствию необходимости инсталлировать дополнительные программные и аппаратные средства, а также своей мобильности. Защита систем «Банк–Клиент».

Особенностью защиты «толстого» решения является наличие на рабочем месте клиента установленного комплекта ПО, состав которого определяет сам банк. То есть у кредитно-финансовой организации есть возможность выдвинуть ряд требований к программному обеспечению на конечной рабочей станции. Вводить в состав системы «Банк–Клиент» решение по endpoint-защите стало хорошей практикой в банковской среде. Из наиболее часто применяемых методов здесь – пассивный мониторинг активности в программной среде или даже комплексное решение, которое может включать в себя такие модули, как антивирусное ПО, хостовый IPS, базовый персональный межсетевой экран, средства криптографической защиты информации (СКЗИ), возможность многофакторной аутентификации и т.д. [13, стр. 117].

Практика использования традиционных средств защиты банк-клиентов это кроме применения криптосредств для защиты передачи информации по недоверенным каналам связи использование сертифицированных ФСБ СКЗИ

для генерации электронных цифровых подписей (ЭЦП). Основная задача криптосредства в данном случае – обеспечение неотказуемости банковских операций в случае возникновения конфликтов (использование сертифицированных средств позволяет обеспечить юридическое основание при рассмотрении спорных случаев в судебных инстанциях). Защита ключевой информации. Использование СКЗИ и ЭЦП для совершения банковских операций означает, что ключевая информация является в подобных системах «Клиент–Банк» одним из главных объектов атаки. Обладая этими данными, нарушитель сможет совершать легитимные финансовые транзакции от лица клиента.

В связи с этим дополнительные меры для защиты ключевой информации всегда являются приоритетными. Среди основных тенденций – уход от применения накопителей и использование различных защищённых способов хранения информации, а также исключение ее хранения в недоверенной среде. Например, желательно использование процессорных смарт-карт и USB-токенов с возможностью совершения криптоопераций непосредственно на аппаратном устройстве. Двухфакторная аутентификация. Дополнительным уровнем защиты может быть двухфакторная аутентификация сессии работы пользователей с системой «Клиент–Банк». Для этого можно использовать аппаратные и программные генераторы одноразовых паролей, токены и т.д. Аутентификация на уровне транзакций. Проверка подлинности предполагает не единичную аутентификацию в рамках сессии работы системы «Банк–Клиент», а проверку при каждой из финансовых операций. Эта технология всегда способствует повышению уровня защищённости, но очень редко применяется для корпоративных клиентов. Дело в том, что при проведении большого количества платежей подобный режим вызывает слишком большое число нареканий со стороны самих пользователей системы. Антивирусное ПО. Так или иначе, вредоносный код – это основной вектор атаки, в том числе и для

корпоративных клиентов. Поэтому рекомендации по использованию комплексов антивирусной защиты на компьютерах с ДБО предлагаются практически всегда. Иногда в практике защиты встречаются случаи, когда антивирусная защита (хотя бы бесплатная) включается непосредственно в комплект поставки ПО «Клиент–Банк». Использование комплексов End - point Security. Дополнительным уровнем защиты от внешнего воздействия систем «Клиент–Банк» является использование автономно управляемых (зачастую с предустановленными рекомендованными настройками) комплексов Endpoint Security. Кроме антивирусной защиты, они могут включать в себя один или несколько компонентов: персональный межсетевой экран, хостовое средство обнаружения вторжения, средство криптографической защиты. Защита web-банкинга. В случае web-банкинга всё богатство мер, традиционно используемых для защиты ДБО, оказывается, в лучшем случае, трудно применимым. Здесь преимущества web-технологий играют злую шутку. Отсутствие жёстких требований к программной платформе и инсталлируемого софта накладывает ограничения на защиту со стороны клиента. При этом риски для этой категории наиболее высоки.

Традиционные средства защиты предлагают для web-банкинга это использование протокола SSL, который позволяет обеспечить проверку подлинности сервера и шифрование сессии. Он применяется повсеместно в связи с тем, что реализован во всех современных браузерах, и позволяет избежать большого количества достаточно простых атак, таких как перехват аутентификационных данных или простые решения класса Man-in-the-Middle. В то же время протокол не обеспечивает защиту при компрометации браузера или подмене сертификатов корневых удостоверяющих центров на клиентских местах. Существуют также версии протокола с определенными слабостями и уязвимостями. Защита от логирования данных доступа, которая подразумевает использование «виртуальных клавиатур», капч и других

способов борьбы с перехватом и/или автоматизированным подбором аутентификационной информации. Однако, постоянное развитие вредоносного кода и различных систем логирования активности пользователя делает эти меры недостаточными, и их применение при построении систем web-банкинга не требует больших расходов и потому может рекомендоваться для использования [39,стр.36].

Прежде всего, используются решения с низкой стоимостью владения в пересчете на отдельного пользователя. Это блокноты с одноразовыми паролями, SMS-аутентификация или аутентификация с использованием ПО на мобильных устройствах (смартфонах, коммуникаторах, планшетах). Иногда возможно применение цифровых сертификатов на различных носителях, систем генерации одноразовых паролей и даже биометрии. Но эти решения подразумевают высокие накладные расходы, как правило, ложащиеся на плечи клиентов при подключении к web-банкингу и потому применимые только в ограниченных случаях (к примеру, для VIP и имиджевых клиентов). Кроме того, некоторые из систем многофакторной аутентификации накладывают дополнительные ограничения на используемые платформы, что может сводить на нет преимущества web-банкинга для клиентов. В текущий момент наиболее популярным вариантом многофакторной аутентификации при доступе является именно SMS-аутентификация. Она предполагает достаточный уровень защиты при минимальных затратах и хорошо масштабируется (можно привести пример компании Google, использующей этот метод для доступа пользователей к сервису Gmail). Однако, по сообщениям McAfee Labs, новые версии вредоносного ПО уже научились компрометировать SMS-аутентификацию в ДБО путем реализации атаки Man-in-the-Middle прямо на коммуникаторе пользователя. Учитывая, что доля смартфонов и коммуникаторов растёт, а аудитория, активно использующая мобильные технологии, в достаточной степени совпадает с контингентом пользователей веб- и мобильного

банкинга, число атак, реализуемых посредством компрометации смартфонов, будет только расти.

Дополнительной мерой защиты может выступать использование многофакторной аутентификации не для получения доступа к системе web-банкинга, а для авторизации отдельных транзакций во время работы с ней. Способ обеспечивает частичную защиту от вредоносного ПО, работающего в уже открытой сессии пользователя. Для клиентов–физических лиц (в отличие от юридических) эта защита может считаться приемлемой ввиду удобства ее реализации: количество финансовых транзакций в рамках одной сессии в данном случае редко бывает значительным. Оповещения о проведённых транзакциях. SMS и E-mail оповещения клиента о каждой транзакции могут также рассматриваться как средства борьбы с различными методами перехвата сессий работы с web-банкингом (хотя бы с точки зрения минимизации возможных потерь). Поэтому клиент всегда узнает о начале неправомерного использования его учётных данных. Кроме того, в соответствии с положениями нового закона ФЗ-161, отсутствие уведомления клиента о совершённой транзакции рассматривается как безусловное перенесение ущерба от мошеннических операций на сторону банка.

ИБ на рынке имеется достаточно широкий спектр решений, которые позволяют обеспечить эффективную защиту систем ДБО. Наряду с традиционными межсетевыми экранами, антивирусами, системами обнаружения атак и т. п. есть и специализированные продукты, к которым он относит инструменты усиленной аутентификации, системы мониторинга банковских транзакций с целью выявления мошенничества, а также средства создания доверенной среды ДБО. Некоторые российские компании, работающие на рынке ИБ, начали предоставлять консалтинговые услуги по проведению аудита информационной безопасности ДБО-систем. В рамках такого аудита проверяется устойчивость системы к возможным атакам

злоумышленников, а по результатам формируется отчет с описанием выявленных уязвимостей и рекомендациями по их устранению [16, стр.36].

По мнению Сергея Котова, была, есть и будет необходимость в разработке и использовании принципиально новых методов и продуктов для обеспечения безопасности ДБО, которые должны следовать за развитием сервисов ДБО и технологий, используемых киберпреступниками. Разработчикам систем ДБО и ДБО-провайдерам он рекомендует уделять внимание не только функциональности систем, но и безопасности их использования. На первый план в защите ДБО должно, как он считает, в скором времени выдвинуться страхование ИБ-рисков кредитно-финансовыми учреждениями (но не клиентами) [67].

На взгляд Евгения Афонина, инструменты, необходимые для обеспечения защиты ДБО, уже придуманы, и задача заключается в том, чтобы их правильно использовать. Большей эффективности, утверждает он, можно добиться за счет риск-аналитического подхода, если положить его в основу управления информационной безопасностью ДБО. Повысить уровень защиты систем ДБО, по его мнению, можно, применяя поведенческий анализ действий пользователей и профилирование выполняемых ими транзакций [66].

Как полагает Алексей Сизов, в краткосрочной перспективе для защиты ДБО нужно сосредоточиться на средствах защиты клиентской среды. К ним он относит механизмы интеллектуального реагирования на факты мошенничества и инструменты усиленной аутентификации пользователей, подтверждающие легитимность операций ДБО. В настоящее время на стороне ДБО-провайдера для этого используют как специализированные системы антифрода, так и настройки на отработку событий, связанных с мошенничеством, системы управления информационной безопасностью (СУИБ). В среднесрочной перспективе внимание будут уделять механизмам защиты и контроля программного обеспечения систем ДБО, а также

контролю действий обслуживающего персонала (сотрудников банков, аутсорсинговых компаний и т. д.) [64].

Андрей Голов наиболее эффективным подходом к обеспечению безопасности ДБО считает внедрение защиты внутри самой ДБО-системы. На его взгляд важно, чтобы используемые средства криптозащиты ДБО и критичные части самой системы ДБО функционировали в единой защищённой среде. Однако если обеспечивать неизвлекаемость ключевой информации в каком-либо отдельном носителе, то необходимо, чтобы и криптографические операции тоже выполнялись в этом носителе, и визуализация информации защищаемых процессов была реализована на нём же. При пакетной обработке транзакций, когда невозможно выполнить ее визуализацию рекомендуется использовать такие приемы, как “белый список” надёжных получателей, управление рисками выполнения операций и т. п. [65].

Подходы к обеспечению ИБ в системах ДБО нужно пересматривать, двигаясь в двух направлениях. Во-первых, часть системы банк — клиент следует поместить в доверенную среду, которая реализуется вне операционной системы на защищенном внешнем носителе. Это должно обеспечить целостность и неизменность платежных документов во время их подписания. Подобный подход может потребовать дополнительной стоимости. При этом Банк готов потратить на защиту одного клиентского средства доступа к системе ДБО не более ста долларов. Это заставляет ИБ-разработчиков применять решения класса Trusted Screen, представляющие собой аппаратные устройства размером с ладонь с сенсорным экраном, в доверенной среде которых подписывается документ и отображаются платежные данные. К недостаткам этого подхода можно отнести необходимость применять дополнительное устройство, а также дорогие токены и смарт-карты со встроенной криптографией.

Второй компромиссный вариант защиты платежных документов от фальсификаций представляет собой тонкий или доверенный клиент, разворачиваемый на клиентском компьютере в виде виртуальной машины, на которой создается доверенная среда для просмотра и подписи платежных документов. Такое решение не требует дополнительных устройств, кроме доверенного носителя. Однако пользователь, работая с системой ДБО в такой среде, сильно ограничен, так как система “не видит” ресурсов рабочей стации и не может с ними работать.

Совмещение упомянутых выше двух подходов позволяет обойти их недостатки. Суть такого совмещения заключается в том, что до загрузки вычислительной системы клиентского рабочего места некоторые ее ресурсы (одно ядро процессора, часть памяти и ресурсов видеокарты и т. д.) занимается микрокодом доверенной среды и пользовательскими ключами. После выполнения этой процедуры стартует загрузка операционной системы компьютера, которая теперь “не видит” “изъятых” у нее ресурсов и не может к ним обращаться. Благодаря этому никакие вредоносные программы не в состоянии перехватить критические данные, которые загружены в сформированную таким способом доверенную среду.

Когда в системе ДБО проводится банковская транзакция, внедренный микрокод переключает компьютер в доверенную среду, отображает документ на экране компьютера, затем формирует электронную подпись и возвращает управление операционной системе. Эта технология отличается надежностью, низкой стоимостью, не требует дополнительных устройств для совершения операций и визуализации.

Таким образом, теоретически обоснованы, и практически реализуются методические подходы обеспечения информационной безопасности дистанционного банковского обслуживания. Факторы, затрудняющие защиту, исследуем детально в следующем пункте нашей работы.

## 1. 3. Внешние и внутренние факторы, затрудняющие защиту дистанционного банковского обслуживания

Развитие информационных технологий в банковском деле предопределило появление рынка электронных банковских услуг, отличающихся новыми стандартами проведения операций и качеством обслуживания, что предоставляет новые возможности привлечения и удержания клиентов банков. Переход банков к клиентоориентированным стратегиям на сегодня имеет много последствий. Прежде всего, он затронет сферу управления коммерческой информацией, позволяя банкам проводить более продуманную политику привлечения и удержания клиентов. Ускоряется разработка новых продуктов и услуг, связанных с новыми технологиями, расширяется использование виртуальных каналов сбыта, изменится политика ценообразования, клиенты будут получать качественные услуги в режиме онлайн и т. д. Все это увеличивает риски информационной безопасности, способствует разработке и становлению новой системы информационной безопасности дистанционного банковского обслуживания.

В настоящее время наметилась тенденция роста мошеннических действий, возникающих в банковской сфере, что подрывает все основы экономической жизни страны.

Из новостных сводок мы все чаще слышим о масштабных операциях против кибермафии, которые проводятся почти во всех российских регионах. Хакерские группировки, используя различные криминальные схемы, в буквальном смысле слова могут обнулять банковские счета за считанные минуты. Это наносит колоссальный ущерб как клиентам банка (физическим и юридическим лицам), самим кредитным организациям, так и всей отечественной банковской системе. К прямому ущербу относится сумма всех похищенных денежных средств, вне зависимости от того, кто в конечном итоге понес убытки – кредитная организация или клиент.

По официальным заявлениям МВД России «помимо незаконного проникновения в банковские системы, опасность злоумышленников заключается во взломе объектов критической важной инфраструктуры, в том числе объектов транспорта и стратегических промышленных предприятий Российской Федерации».

Убытки банков от мошеннических операций исчисляются миллиардами рублей. Чаще всего проведение таких операций осуществляется в результате взлома систем дистанционного банковского обслуживания (ДБО). В настоящий момент объем ущерба от мошенничества в системах ДБО превышает 100 млн. долларов.

Однако по прогнозам экспертов, непосредственно участвующих в расследованиях инцидентов в ДБО как со стороны кредитных организаций, так и правоохранительных органов, динамика потерь от мошеннических операций в ближайшие годы будет только увеличиваться. На это влияет одновременно 2 фактора: вызванное экономическим кризисом сокращение инвестиций в информационную безопасность со стороны банков РФ и широкое распространение средств совершения киберпреступлений [63].

Банки являются для хакеров «самым лакомым куском», так как там есть самое главное, за чем они охотятся — деньги. Эксперты по кибербезопасности объясняют мошеннические схемы следующим образом: преступники внедряют в сеть банка-жертвы вредоносные программы, с помощью которых похищают данные, вмешиваются в работу и, соответственно, похищают деньги. Эти программы еще называют «троянскими», потому что хакеры маскируют их под деловые или личные письма. Кто-то из сотрудников банка в большинстве случаев должен активизировать эту вредоносную программу. В связи с этим особое внимание следует уделять обучению и своевременному инструктажу банковских сотрудников по требованиям систем безопасности.

Денежные средства крадут и у обычных людей — с банковских карт, и со счетов финансовых организаций. Причем в последнем случае за одну атаку мошенники могут увести очень крупные суммы. Поэтому обоснованным является регулярное ужесточение требований Центробанка по внутренней безопасности для финансовых организаций. Все банки должны понимать важность и нужность вопросов информационной безопасности, соблюдать требования, которые Центральный банк выставляет с точки зрения защиты информации и безопасности. Поэтому совершенствование системы банковской безопасности посредством внесения коренных изменений в нормативно-правовое регулирование в ближайшее время станет для Российской Федерации первостепенной задачей.

Физическим лицам – клиентам банков эксперты рекомендуют не посещать сомнительные сайты, не открывать подозрительные электронные письма, на мобильные устройства загружать только официальные банковские приложения. Ведь мошенники, как и человечество в целом, все глубже уходят в интернет.

Защита ДБО является задачей комплексной и должна реализовываться как на стороне кредитно-финансовой организации, так и на стороне клиента. Большинство успешных атак на системы ДБО проводится через плохо защищенные клиентские места, на которых не выполняются даже базовые требования по защите информации. Отсутствие должного внимания к проблеме защиты информации со стороны клиентов ДБО является одним из основных факторов, затрудняющих эффективную защиту системы.

Проблемы обеспечения ИБ, а именно невозможность для провайдера реализовать и гарантировать требуемую безопасность на стороне клиента, а для клиента — организовать адекватный контроль за качеством услуги (включая ее безопасность) на стороне провайдера.

Первый фактор для ДБО играет сегодня более значимую роль, и поэтому клиенты, по мнению экспертов, остаются наиболее уязвимым звеном в обеспечении безопасности ДБО.

Второй фактор в основном связан с доступностью сервиса, и возникающие в этой связи проблемы могут быть разрешены сменой ДБО-провайдера (рис. 1.3).

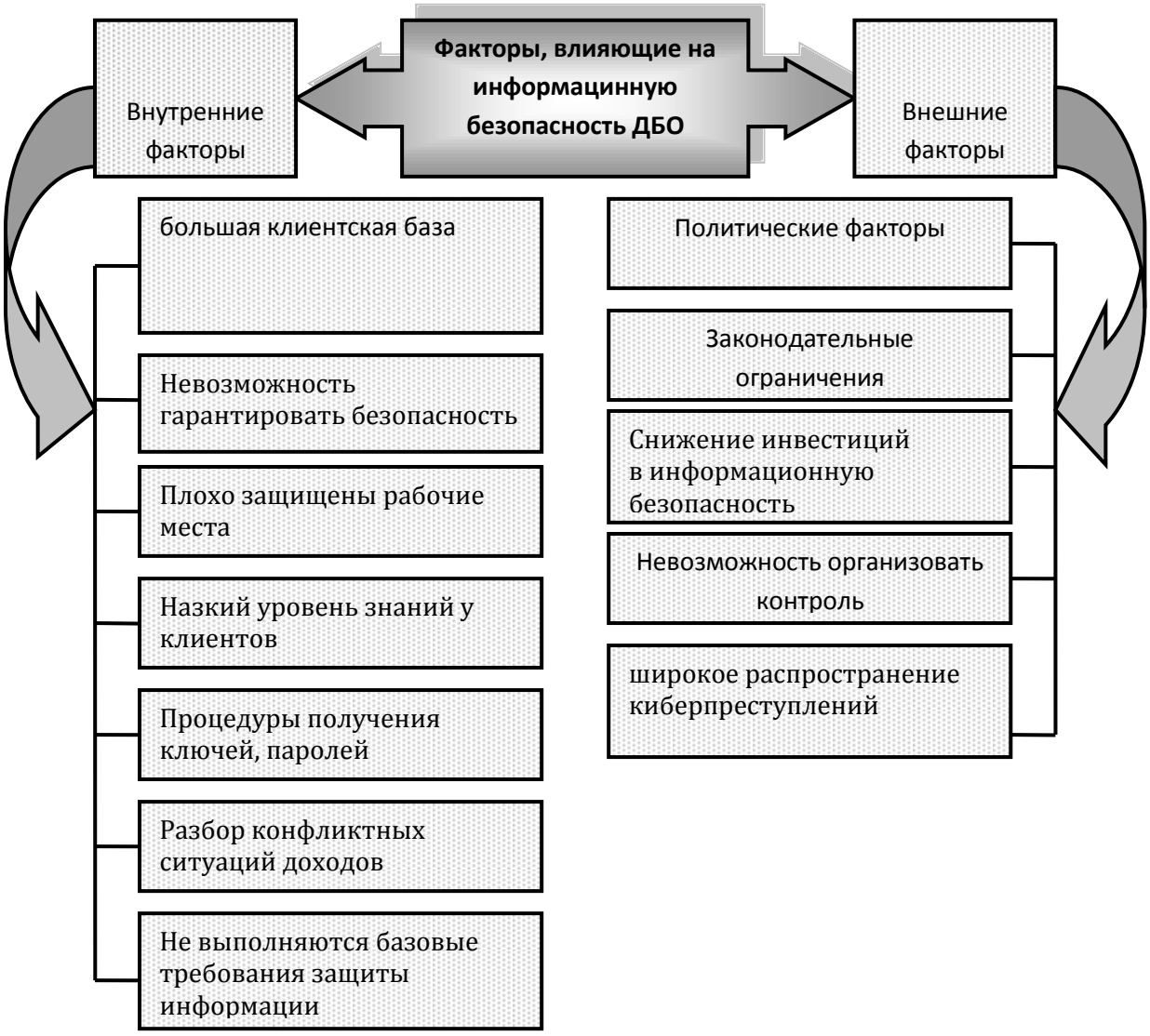


Рис.1.3. Факторы, затрудняющие обеспечение информационной безопасности

К факторам, затрудняющим обеспечение ИБ систем ДБО, эксперты относят также высокие требования со стороны клиентов к удобству эксплуатации таких систем. Процедуры получения ключей электронной подписи, их применения, разбор конфликтных ситуаций и т. п. не должны быть сильно обременительными для пользователей.

Использование средств защиты ДБО затрудняется также длительным процессом внедрения, что связано с большой и распределенной клиентской базой ДБО-систем. Внедрение системы защиты может приводить к значительной модификации самих систем ДБО в целом. К управлению системами ДБО пока привлекают в основном специалистов службы ИТ, игнорируя ИБ-службу, что также не способствует безопасности ДБО-услуг.

Виктор Сердюк полагает, что для эффективного противодействия атакам на системы ДБО помимо использования современных средств и методов защиты необходимо налаживать более тесное взаимодействие между банками, правоохранительными органами, регуляторами, а также компаниями, работающими на рынке защиты информации. В настоящее время эта задача, по его наблюдениям, решается путем создания специализированных профессиональных ассоциаций и рабочих групп, в рамках которых обсуждаются проблемы защиты систем ДБО и возможные пути их решения [60].

Поскольку конкуренция на рынке услуг ДБО ощущается уже весьма остро, стоимость для клиента защиты как дополнительного сервиса не должна быть высокой. В противном случае повышается срок самоокупаемости ДБО-систем, что не стимулирует банки рассматривать ИБ как конкурентное преимущество в сфере услуг ДБО.

Совокупность внешних и внутренних условий защиты дистанционного банковского обслуживания, специфические закономерности в значительной мере оказывают влияние на результаты деятельности ПАО Сбербанк.

# ГЛАВА 2. СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (НА ПРИМЕРЕ ПАО Сбербанк)

## 2.1. Организационно-экономическая характеристика ПАО Сбербанк

Акционерный коммерческий Сберегательный банк Российской Федерации (ПАО Сбербанк), именуемый в дальнейшем «Банк» был основан в 1841 г. Банк создан в форме акционерного общества в соответствии с Законом РСФСР "О банках и банковской деятельности в РСФСР" от 2 декабря 1990 г. и зарегистрирован 20 июня 1991 г. Место нахождения Банка: Россия, 117997, город Москва, улица Вавилова, дом 19. Согласно Уставу, учредителем банка является Центральный банк Российской Федерации. Акционерами Сбербанка могут быть юридические и физические лица, в том числе иностранные, в соответствии с законодательством Российской Федерации.

Организационная структура ПАО Сбербанка и его центрального аппарата, управление Сбербанком России основывается на принципе корпоративности в соответствии с Кодексом корпоративного управления, утвержденным годовым Общим собранием акционеров Банка. Органы управления Банком формируются на основании Устава ПАО Сбербанка России и в соответствии с законодательством Российской Федерации.

Филиалы Банка (территориальные банки, отделения) не наделены правами юридических лиц и действуют на основании Положений, утверждаемых Правлением Банка, имеют печать с изображением эмблемы Банка со своим наименованием, а также другие печати и штампы, имеют баланс, который входит в баланс Банка. Изменения в Устав, связанные с открытием, закрытием филиалов и изменением их статуса, вносятся по

решению Наблюдательного совета Банка не реже 1 раза в год.

Сбербанк наращивает свое присутствие и на новых сегментах рынка банковских услуг для физических лиц. Банк является участником международных платежных систем. Выпускает и обслуживает пластиковые карточки: VISA (Classic, Gold, Business) и карточки Eurocard / Mastercard (Mass, Gold, Business), микропроцессорные пластиковые карточки Сбербанка Сберкард.

Публичное акционерное общество «Сбербанк России» является крупнейшим российским банком и среди них занимает 1 место по активам-нетто. На 01 января 2016 г. и 2017 г. доля активов-нетто банка Сбербанк России составила 28,9%. Только за год активы увеличились на 5,60%. Прирост активов-нетто отрицательно повлиял на показатель рентабельности активов ROI, который упала с 2,17 % до 1,28%. Рейтинги показаны в табл.2.1

Таблица 2.1

Рейтинги, присвоенные Сбербанку международными агентствами по состоянию на 01.01 2017-2018 годы

| Показатели | на 01.01.2017 г | | на 01.01 2018 | |
|---|---|---|---|---|
| | Fitch Ratings | Moody’s | Fitch Ratings | Moody’s |
| Долгосрочный рейтинг в иностранной валюте: | | | | |
| Сбербанк | BBB- | BA2 | BA1 | BA2 |
| Российская Федерация | BBB- | BA1 | BA1 | BA1 |
| Рейтинг международных обязательств<br>Ноты участия в кредитах, выпущенные в рамках MTN-программы, Сбербанка<br>Еврооблигации Российской Федерации | <br><br>BBB-<br><br>BBB- | <br><br>BA1<br><br>BA1 | <br><br>BBB-<br><br>BBB- | <br><br>BA1<br><br>BA1 |

Сбербанк сохранил лидирующие позиции на всех основных сегментах финансового рынка Российской Федерации. Прогноз макроэкономических показателей и банковского сектора на 2018 год. Базовый сценарий на 2018 год предполагает стабилизацию цен на нефть на уровне 62 доллара США за баррель марки Urals. Согласно базовому сценарию, рост экономики составит

2%, средний курс доллара – 58 рублей, инфляция на конец года – 4%, ставка Банка России на конец года – 6,75%.

Таблица 2.2

Доля ПАО Сбербанк в основных сегментах российского финансового рынка в 2016-2017 годы, %

| Показатели | 2016 г. | 2017 г. | Изменение %, +,- |
|---|---|---|---|
| Активы | 28,9 | 28,9 | - |
| Кредиты корпоративным клиентам | 31,7 | 32,4 | 0,7 |
| Кредиты частным клиентам | 40,1 | 40,5 | 0,4 |
| Средства корпоративных клиентов | 22,1 | 20,9 | -1,2 |
| Средства частных клиентов | 46,6 | 46,1 | -0,5 |
| Капитал | 33,5 | 39,3 | 5,8 |

ПАО Сбербанк осуществляет свою деятельность на основании Генеральной лицензии на банковские операции №1481, выданной Банком России 11 августа 2015 года. Сбербанк также имеет лицензию на осуществление банковских операций на привлечение во вклады и размещение драгоценных металлов, другие операции с драгоценными металлами, лицензия профессионального участника рынка ценных бумаг на ведение брокерской, дилерской, депозитарной деятельности, а также на деятельность по управлению ценными бумагами.

Основной деятельностью Сбербанка являются следующие банковские операции:

К первому направлению операций относится обслуживание расчетных и текущих счетов, открытие депозитов, предоставление финансирования, выдача гарантий, обслуживание экспортно-импортных операций, инкассация, конверсионные услуги, денежные переводы в пользу юридических лиц и др.

Операции с розничными клиентами: принятие средств во вклады и ценные бумаги Банка, обслуживание банковских карт, кредитование, платежи, денежные переводы, купля-продажа иностранной валюты,

операции с драгоценными металлами, хранение ценностей и др.

Операции на финансовых рынках: с ценными бумагами, производными финансовыми инструментами, иностранной валютой и др.

Таблица 2.3

Показатели выполнения нормативов ликвидности Сбербанка

| Нормативы ликвидности | Предельное значение, установленное Банком России,% | Критическое значение Сбербанка,% | Значения норматива на отчетную дату,% | | Соответствие требованиям Банка России |
|---|---|---|---|---|---|
| | | | 01.01.2017 | 01.01.2018 | |
| Н2 | Мин 15 | Мин 20 | 217,0 | 161,89 | соответствует |
| Н3 | Мин 50 | Мин 55 | 301,6 | 264,90 | соответствует |
| Н4 | Макс 120 | Макс 115 | 55,4 | 57,52 | соответствует |

Приведенные данные в таблице 2.3 нормативов ликвидности по итогам за два года показывают выполнение предельных значений обязательных нормативов установленных Банком России, так и внутренние критические значения нормативов, установленные Сбербанком с запасом в целях управления рисками ликвидности.

Исходя из данных, представленных в таблице 4, можно сделать вывод, что в анализируемом периоде наибольший удельный вес в совокупных активах ПАО Сбербанк, как и ранее, занимают чистая ссудная задолженность и чистые вложения в ценные бумаги. При этом эти показатели имеют тенденцию к увеличению их доли в структуре в 2016 году на 0,39 % чистой ссудной задолженности и на 0,35% чистые вложения в ценные бумаги. Коммерческие банки выполняют особую роль в экономике – занимаются перераспределением капитала, отсюда большую часть активных операций составляют кредитные 74,68%.

Развитие финансовых рынков, в том числе рынка ценных бумаг способствует использованию его финансовых инструментов в усилении конкурентных позиций компаний и их стоимости, улучшения качества активов. Структура активов и пассивов ПАО Сбербанк за период 01.01.2016–2018 гг. приведена в таблице 2.4.

Таблица 2.4

Структура активов и пассивов ПАО Сбербанк на 01.01.2016– 2018 гг.

| Наименование статьи | на 01.01.2016 г. | | на 01.01.2017 г. | | на 01.01.2018 г. | | Изм. % за год, +,- |
|---|---|---|---|---|---|---|---|
| | млн. руб. | % | млн. руб. | % | млн.руб. | % | |
| Денежные средства | 732789,74 | 3,23 | 614848,98 | 2,83 | 621 718,6 | 2,5 | - 0,33 |
| Средства в Центральном Банке РФ | 586685,38 | 2,59 | 967161,87 | 4,45 | 747 906,5 | 2,4 | - 2,05 |
| Средства в кредитных организациях | 355984,91 | 1,56 | 347942,78 | 1,60 | 312 12,0 | 1,3 | - 0,3 |
| Финансовые активы, оцениваемые по справедливой стоимости | 405977,87 | 1,79 | 141343,23 | 0,65 | 91 469,0 | 0,1 | - 0,55 |
| Чистые вложения в ценные бумаги и др. финансовые активы, имеющиеся в наличии для продажи | 2316356,73 | 10,20 | 2269613,00 | 10,45 | 2 537 280,1 | 10,8 | + 0,35 |
| Чистые вложения в ценные бумаги, удерживаемые до погашения | 455961,16 | 2,00 | 436472,31 | 2,01 | 645 442,1 | 2,7 | + 0,69 |
| Чистая ссудная задолженность | 16869803,46 | 74,29 | 16221622,14 | 74,68 | 17 456 305,3 | 75,9 | + 1,22 |
| Основные средства, материальные запасы | 467474,01 | 2,06 | 469120,69 | 2,15 | 481 454,5 | 1,7 | - 0,45 |
| Прочие активы | 515882,83 | 2,28 | 252953,48 | 1,18 | 327 361,4 | 0,2 | - 0,98 |
| Всего активов | 22706916,09 | 100 | 21721078,48 | 100 | 23 234 932,0 | 100 | - |
| Средства Центрального Банка РФ | 768989,23 | 3,38 | 581160,31 | 2,68 | 591 164,2 | 2,4 | - 0,28 |
| Средства кредитных организаций | 618363,82 | 2,72 | 364499,53 | 1,67 | 464 229,7 | 4,3 | + 2,63 |
| Средства клиентов | 17722423,46 | 78,05 | 16881988,99 | 77,72 | 18 102 308,6 | 72,7 | - 5,02 |
| Выпущенные долговые обязательства | 647694,36 | 2,85 | 610931,89 | 2,81 | 215 723,0 | 2,4 | - 0,41 |
| Прочие обязательства | 256566,98 | 1,13 | 280194,32 | 1,28 | 261 526,8 | 0,5 | - 0,78 |
| Резервы на прочие потери | 37805,39 | 0,17 | 42145,67 | 0,19 | 135 067,1 | 2,9 | +2,71 |
| Источники собственных средств | 2328152,61 | 10,25 | 2828920,89 | 13,02 | 3 380 793,7 | 13,8 | + 0,78 |
| Прочие пассивы | 326920,24 | 1,45 | 131236,88 | 0,63 | 3 118 073 | 0,0 | - 0,63 |
| Всего пассивов | 22706916,09 | 100 | 21721078,48 | 100 | 24 415 430,2 | 100 | - |

Наибольший удельный вес в его структуре пассивов занимают средства клиентов, а также источники собственных средств. Доля первого показателя в 2018 г. составила 72,7%, что в сравнении с предыдущим отчетным периодом произошло уменьшение его в структуре на 5,02%. Сбербанк в качестве приоритетов выделяет формирование источников финансирования

активов за счет собственных средств, доля которых увеличивается и составляет на 1 января 2018 года 13,08%.

Основные результаты деятельности ПАО Сбербанк за 2016 год в сравнении с 2014 годом представлены в таблице 2.5.

Таблица 2.5

Абсолютные показатели деятельности ПАО Сбербанк

за 01.01.2016 – 2018 гг., млн. руб.

| Показатели | 01.01.2016г | 01.01.2017г | Темп прироста, % | 01.01.2018г | Темп прироста, % |
|---|---|---|---|---|---|
| Процентные доходы всего | 1 958 101,6 | 2 048 850,3 | 4,43 | 1996 745,2 | -2,54 |
| Процентные расходы | 1132322,5 | 876 427,7 | -22,5 | 727 768,2 | -16,96 |
| Чистые процентные доходы (отрицательная процентная маржа) | 825 779,1 | 1172422,6 | 41,9 | 1268977,0 | 8,23 |
| Расходы на формирование (Доходы от восстановления (+) резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности, средствам, размещенным на корреспондентских счетах, а также начисленным процентным доходам | -293903,1 | -114783,4 | -60,9 | - 114 912,2 | - 0,11% |
| Чистые доходы (расходы) | 1268474,2 | 1566730,4 | 23,5 | 1576892,5 | 0,64 |
| Операционные расходы | 952015,1 | 871652,6 | -8,4 | 702091,6 | -0,19 |
| Прибыль (убыток) до налогообложения | 316459,1 | 695077,9 | 119,6 | 874 801,0 | 25,85 |
| Прибыль (убыток) за отчетный период / Прибыль (убыток) после налогообложения | 236256,2 | 516987,8 | 118,8 | 674119,8 | 30,39 |
| Финансовый результат за отчетный период | 218 387,0 | 576 834,5 | 164,1 | 715 036,9 | 23,95 |

В структуре привлеченных ресурсов наибольший удельный вес

составляют вклады населения. Традиционно, ориентируясь на работу с населением, Сбербанк России является абсолютным лидером на рынке частных вкладов, размещенных частными лицами в коммерческих банках стран. Сбербанк России предлагает частным лицам широкий спектр банковских услуг, разнообразные виды рублевых и валютных вкладов, ориентированные на различные слои населения.

Оптимизированы расходы на поддерживающие сервисы. В 2017 году чистая прибыль составила 748,7 млрд. руб., рост в 2,1 раза к 2013 году, 24% рентабельность собственного капитала (Return on Equity) в 2017 году, 35% отношение операционных расходов к операционным доходам до резервов (Cost-to-Income ratio) в 2017 году 11,4% достаточность основного капитала 1-го уровня, Базель 3.

Таким образом, умелое использование Банком своих преимуществ, активное развитие новых продуктов и услуг позволили добиться по итогам 2017 года значительных финансовых результатов, повысить эффективность отдельных операций, увеличить объёмы бизнеса в отдельных сегментах и сохранять лидерство в банковской сфере по всем основным показателям.

## 2.2. Особенности формирования системы информационной безопасности дистанционного банкоского обслуживания

ПАО Сбербанк особое значение отводит технологическому прорыву, и на сегодня созданы основы технологической платформы: завершено формирование технологических компонентов ядра, созданы инструменты разработки бизнес-сервисов и начат перевод первых продуктов банковского бизнеса на новую платформу. Созданы системы работы с данными и аналитикой: заложены основы инфраструктуры хранения и обработки

данных на базе «облачных» технологий, запущена Академия технологий и данных в Корпоративном университете, началось внедрение технологий искусственного интеллекта. Повышена отказоустойчивость ИТ-систем.

Обеспечен высокий уровень кибербезопасности бизнеса, несмотря на общий рост количества киберпреступлений в отрасли. Упрощен и унифицирован ИТ-ландшафт банка, завершено строительство нового центра обработки данных «Сколково» 700 нецелевых автоматизированных систем было выведено из эксплуатации, в 20 раз снижены простои автоматизированных систем, 99,99% уровень надежности для критических автоматизированных систем в режиме 24/7, в 57 раз выросло количество big data-инициатив с 10 в 2016 году до 575 в 2017 году, 1 место банка в рейтинге крупнейших разработчиков программного обеспечения по версии CNEWS.

Таблица 2.6

Количество активных пользователей ПАО Сбербанк в 2017г.

| Показатели | Физические лица | Юридические лица | Откл.,раз |
|---|---|---|---|
| Ежемесячные активные пользователи (MAU), млн. | 50,4 | 1,63 | 30,9 |
| Ежедневные активные пользователи(DAU),млн. | 14,6 | 0,784 | 18,6 |
| Отношение ежедневных пользователей к ежемесячным, % | 29 | 48 | -1,66 |

Стремясь сделать обслуживание более удобным, современным и технологичным, Сбербанк с каждым годом все более совершенствует возможности дистанционного управления счетами клиентов. В банке создана система удаленных каналов обслуживания, в которую входят:

- мобильные приложения Сбербанк Онлайн для смартфонов (более 31 млн. активных пользователей);
- веб-версия Сбербанк Онлайн (16 млн. активных пользователей);
- SMS-сервис «Мобильный банк» (более 23 млн. активных пользователей);

– одна из крупнейших в мире сетей банкоматов и терминалов самообслуживания (более 90 тыс. устройств).


Рис. 2.1. Каналы обслуживания физических лиц в ПАО Сбербанк в 2017 году

При работе с ДБО применяют способы связи, которые можно разделить на 2 группы: деловой и домашний, их основные отличия представлены в таблице 2.7.

Таблица 2.7

Характеристика видов доступов к банковским услугам через Интернет

| Деловой доступ | Домашний доступ |
|---|---|
| - отражает более 50 операций в одной выписке;<br>- обеспечен многоуровневой защитой;<br>- электронный способ аннулирования платежа;<br>- сортировка операций клиента в зависимости от типа бизнеса. | - доступ только одного владельца;<br>- подключение к системам банка через программу управления наличными средствами;<br>- оплата чеков по сети и телефону;<br>- возможности переводасредств наразличные виды счетов. |

Сбербанк стремится сделать технологические инновации частью собственной ДНК, научиться встраивать их в существующие бизнес-процессы, запускать на их основе новые бизнес-модели.

Технологические инновации позволят сделать ИТ-системы, инфраструктуру и процессы Группы:

— надежными - через обеспечение высокого уровня надежности и доступности всех ИТ-услуг и за счет упрощения архитектуры, централизации и модернизации инфраструктуры;

— гибкими – через обеспечение максимальной скорости вывода продуктов на рынок, увеличение масштабируемости ИТ-систем, упрощение и стандартизацию архитектуры, технологий и процессов;

— эффективными по затратам – благодаря максимальной оптимизации затрат на ИТ и общих расходов бизнеса Сбербанка;

— соответствующими требованиям будущего – благодаря формированию прочного технологического фундамента для дальнейшего

развития банка на срок, превышающий действие новой Стратегии.

Модернизация технологической платформы:

— информационные системы Сбербанка позволяют выдерживать рост транзакционной нагрузки на 40–45 % и пиковой нагрузки на основные системы в среднем на 70 % в год;

— полностью реализована программа централизации ИТ-систем; сегодня Сбербанк строит принципиально новую технологическую платформу, не имеющую аналогов в мире.

Надежность:

— доступность критичных систем Сбербанка составляет 99,99 %;

— более чем в 10 раз снижено время технологических простоев: в 2012 году – 800 часов, в 2016 году – 74 часа;

— почти в 20 раз снижено время простоев из-за инцидентов: в 2012 году – 1056 часов, в 2016 году – 54 часа;

— ЦОД «Южный Порт», введенный в эксплуатацию в 2012 году, сертифицирован по общепризнанным стандартам Tier III и Tier Sustainability GOLD;

— в 2016 году началось строительство ЦОД в инновационном центре «Сколково», который станет крупнейшим в Российской Федерации и одним из крупнейших в Европе. Банк меняет подход в управлении IT-инфраструктурой от принципа доступности ИТ-систем к качеству и надежности бизнес-сервисов.

Гибкость:

— существенно повысилась скорость запуска новых проектов с ИТ-составляющей: с 7 проектов в 2011 году до 270 – в 2016 году.

Эффективность проектов:

— Сбербанк превосходит ведущие мировые банки по ключевым показателям эффективности ИТ (ИТ-расходы, численность и затраты на ИТ-персонал);

— на фоне роста нагрузки стоимость операции неуклонно сокращается.

Операционная модель:

— Сбербанк снизил численность сотрудников, занимающихся сопровождением клиентских операций, с 58 тыс. человек в 2008 году и до 10 тыс. – 2016 году;

— процессы ИТ-сопровождения Сбербанка сертифицированы по CMMI (Level 3);

— проводится Agile-трансформация банка, которая заключается в переходе на метод гибкой разработки («Sbergile»). По ее окончании будут обеспечены максимальная гибкость разработки и максимальная скорость вывода продуктов на рынок.

Супермассивы данных:

— сегодня Сбербанк обрабатывает петабайты (1015) данных;

— анализ больших данных по активности клиентов позволил снизить уровень неработающих кредитов, сократить риски, что, в свою очередь, привело к снижению процентных ставок по кредитам, формированию специальных предложений с более интересными условиями для разных сегментов заемщиков.

Инновации:

— основная стратегическая инновация Сбербанка – создание новой технологической платформы и реализация сервисов на ее основе;

— Сбербанк постоянно исследует появляющиеся технологии с точки зрения возможности их применения и потенциальной пользы;

— основные направления прорывных инноваций в 2016–2017 годах: блокчейн, интернет вещей, машинное обучение, биометрия, облачные вычисления;

— Сбербанк активно вовлекает сотрудников в работу с текущими инновациями: в 2016 году задействовано более 100 тыс. сотрудников, которые подали более 30 тыс. предложений, 13 тыс. из которых были внедрены. Экономический эффект составил более 4 млрд. рублей.

Кибербезопасность:

— запущен базовый функционал Security Operations Center, реализующий систему коллективной защиты банковского сообщества от киберпреступлений в реальном времени в концепции Cyber-Security-as-a-Service;

— более 100 млн транзакций в сутки проверяется онлайн.

Согласно информации, которая содержится в совместном исследовании Lloyd’s of London и Cyence, финансовые потери от масштабной кибератаки могут стоить мировой экономике от 15,6 до 121 млрд. долларов [ ].

Если рассматривать наиболее пессимистический сценарий развития событий, то потери от кибератак могут превысить экономический ущерб от урагана «Катрина», который стал самым разрушительным в истории

Соединенных Штатов. Потери от него составили 108 млрд долларов. Сценарии развития глобальной кибератаки, представлены на рисунке 2.2.

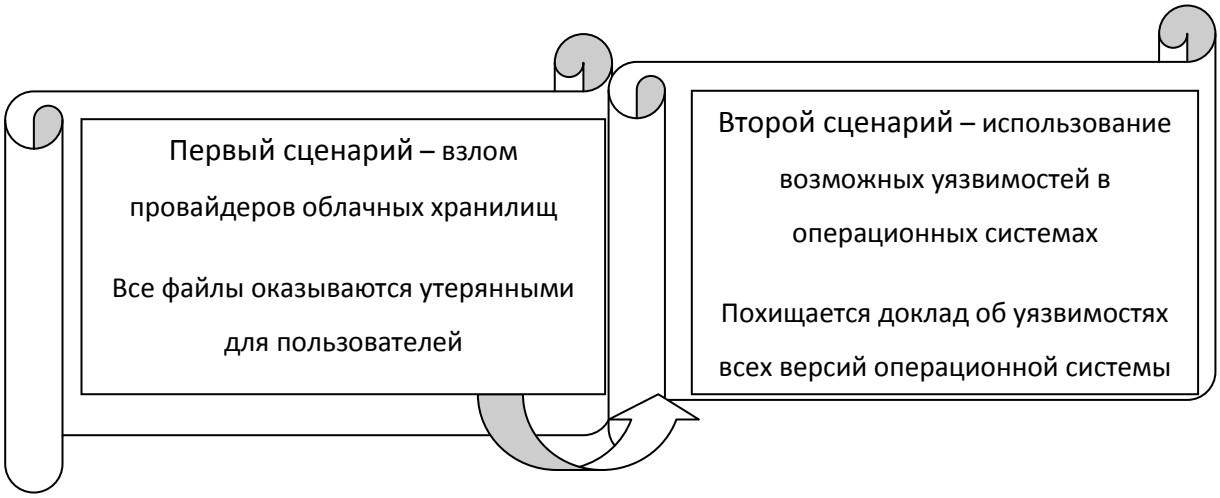


Рис. 2.2. Сценарии развития глобальной кибератаки

Два потенциальных сценария развития глобальной кибератаки: взлом провайдеров облачных хранилищ или использование возможных уязвимостей в операционных системах. В первом сценарии хакеры модифицируют «гипервизор», управляющую систему облачных хранилищ, в результате чего все хранящиеся файлы оказываются утерянными для пользователя. Во втором варианте рассматривается гипотетический случай, когда кибераналитик случайно забывает в поезде сумку, в которой хранится доклад об уязвимостях всех версий операционной системы, установленной на 45 % всех мировых устройств. Этот доклад впоследствии продается в «даркнете» неизвестным криминальным группам.

Минимальный ущерб при первом сценарии составит от 4,6 до 53,1 млрд долларов в зависимости от продолжительности периода недоступности облачных сервисов, а также от того, какие организации подверглись атаке. Эта сумма при определенном, наиболее негативном раскладе может увеличиться до 121,4 млрд долларов. При втором сценарии потери составят от 9,7 до 28,7 млрд долларов.

## 2.3. Характерные признаки киберугроз и риски информационной безопасности дистанционного банковского обслуживания

Проблемы кибербезопасности, особенно в свете недавних масштабных атак на компьютеры предприятий, банков и государственных учреждений, приобрели чрезвычайную актуальность. В нашей стране в последнее время вопросам информационной безопасности (ИБ) в разных секторах экономики, в том числе в финансово-банковском секторе, уделяется особое внимание.

Информационная безопасность складывается из целого комплекса различных мер и действий. Это, прежде всего, контроль действий различных субъектов бизнес-процессов – рядовых сотрудников компании, привилегированных пользователей, ИТ-аутсорсеров, контрагентов. Кроме того, это четкое разграничение прав доступа внутри компании, использование резервного копирования данных, а также наличие простой, понятной и доведенной до сведения работников политики безопасности. В текущих реалиях защита должна быть гибкой, чтобы обеспечить и достаточный уровень защищенности, и выполнение бизнес-целей.

В Банке России считают, что в целом уровень киберустойчивости в нашей стране находится на соответствующем уровне. Также регулятор ожидает снижения количества успешных кибератак и, соответственно, ущерба от них. По итогам первой половины 2017 года количество успешных атак составило порядка 30 % от уровня прошлого года по физическим лицам и порядка 25 % – по юридическим лицам. Например, атака вирусов-шифровальщиков WannaCry и NotPetya практически не коснулась российской финансовой системы. Были единичные случаи заражения информационной инфраструктуры, но это не вызвало негативных последствий – финансово-кредитные организации продолжили свою работу, не было отмечено случаев каких-либо финансовых потерь их клиентов.

Банки вынуждены тратить на кибербезопасность в 3 раза больше, чем остальные компании. Согласно результатам исследования «Лаборатории Касперского», средний годовой бюджет банков на кибербезопасность достигает $58 млн: это в три раза больше, чем у нефинансовых организаций. В большинстве случаев подобные траты оправдываются: представители банков сообщают о значительно меньшем количестве компьютерных преступлений, чем компании такого же размера в других отраслях. Более того, 64% опрошенных заявили, что будут вкладывать в улучшение защиты независимо от окупаемости этих инвестиций.

Рост вложений в киберзащиту имеет веские основания: в последние несколько лет количество угроз для финансовой индустрии неуклонно растет, они становятся все более сложными и чреваты серьезными последствиями, указали в компании. Так, 70% банков сообщили о том, что за последний год они понесли денежные потери в результате кибермошенничества. Больше всего опасений вызывают риски, связанные с мобильным банкингом: 42% респондентов считают, что в ближайшие три года им будет пользоваться подавляющее число клиентов, в то время как уровень киберграмотности пользователей останется низким. Это грозит увеличением количества инцидентов, связанных с кражей денег через мобильные устройства.

Среди других актуальных угроз для пользователей банки выделили фишинг: с ним в 2016 г. сталкивались клиенты 46% компаний. Еще одна сфера повышенного риска — банкоматы. Причем всего 19% банков обеспокоены угрозой атак на них, в то время как в 2016 г. объем вредоносного ПО для банкоматов вырос на 20% по сравнению с 2015 г.

По информации «Лаборатории Касперского», неосторожность пользователей и возрастающее количество атак заставляют банки пересмотреть приоритеты по обеспечению безопасности: 61% участников исследования назвали улучшение защиты приложений и сайтов одним из

главных приоритетов. На втором месте (52%) оказалось внедрение более надежных систем авторизации.

В 2016 г. хакеры похитили с банковских карт россиян 650 млн. рублей. Данный показатель снизился на 15% по сравнению с 2015 годом. Уменьшение количества случаев кражи денежных средств, связано с тем, что держатели карт изучили наиболее популярные схемы мошенничества и научились не реагировать на них. Это следует из расчетов, которые провела компания Zecurion, специализирующаяся на безопасности банковского обслуживания.

В 2017 году объем хищений увеличился до 750 млн. рублей. Кибермошенники совершенствуют свои схемы. Так, злоумышленники звонят гражданам, представляясь сотрудниками банков, и просят сообщить данные карт. Также хакеры крадут данные банковских карт через вирус, рассылаемый в письмах, которые ориентированны на интересы получателей.

В компании подчеркнули, что по итогам текущего года ожидается увеличение объема хищений, так как мошенники ввели новую схему обмана. Они звонят потенциальным жертвам от имени сотрудников Федеральной налоговой службы и под предлогом необходимости погашения задолженности узнают необходимые данные [20, стр. 93].

В 2016 г. количество краж, осуществленных с банковских карт через интернет по вине их владельцев увеличилось на 78% и достигло 107 тыс.

В частности, наиболее распространенным способом мошенничества с пластиковыми картами является атака компьютеров с пользовательскими данными с помощью вирусов-троянов и получение доступа к счету жертвы после незаконного изготовления дубликата ее SIM-карты. В данном случае клиенты виноваты в том, что они пользуются интернет-банкингом на рабочих компьютерах или интегрируют его с социальными сетями.

Также высокую степень риска создает и использование мобильного приложения на смартфоне для входа в личный кабинет интернет-банка —

особенно после выбора четырехзначного кода вместо полноценного логина и пароля для авторизации.

Для защиты своих денежных средств на банковских картах эксперты рекомендуют пользоваться интернет-банком с отдельного компьютера, не хранить на пластиковой карте крупные суммы денег, пополнять баланс карты по мере необходимости, не заходить в интернет-банк через открытые сети Wi-Fi.

Банки долгое время полагали, что АБС находится во внутренней сети и поэтому злоумышленники не смогут до нее добраться. Но сегодня с применением социальной инженерии не представляет большого труда попасть во внутреннюю сеть банка и оттуда успешно атаковать АБС.

19 июля 2016 года созданный Банком России Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) подвел итоги первого года деятельности.

Такие данные опубликованы на открытом заседании Комитета по финансовым рынкам и кредитным организациям Торгово-промышленной палаты РФ. Общая сумма ущерба для банков с января 2016 года исчисляется в размере 2,87 млрд. рублей. Однако, злоумышленникам удалось вывести лишь 1,2 млрд, еще 570 млн удалось остановить и 1,1 млрд заблокировать на счетах кредитных организаций. Александр Чебарь, консультант Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (FinCERT).

В последние два года наблюдается явный вектор смещения атак кибермошенников от клиентов банка в сторону кредитных организаций непосредственно. Это связано, прежде всего, с тем, что в результате целенаправленной атаки на банк преступники получают большую сумму, а процесс ее вывода в последние годы был достаточно простым. Чебарь разъяснил, что в основном использовались карты премиум-сегмента (Visa Gold, Platinum) и сумма входа составляла 2,5 тыс. рублей.

Существуют технологии, которые позволяют предотвратить хищение денежных средств с банковских карт клиентов. В частности, в банковские карты внедряются чипы, значительно снижающие вероятность атаки. Мошенники делают акцент на пользовательские данные клиента (номер карты, CV-код, PIN-код), поэтому при использовании банковской карты требуется внимательность.

Согласно данным, предоставленным коммерческими банками в ЦБ РФ, а также в FinCERT в рамках взаимообмена информацией об инцидентах в области ИБ, в течение 2016 г. общий объем несанкционированных переводов денежных средств, размещенных на банковских счетах, составил в России 1,9 млрд рублей (для сравнения – в 2015 г. этот показатель достигал 3,8 млрд рублей). Специалисты Центрального банка РФ отмечают, что в течение первой половины 2016 года с использованием карт на территории РФ и за ее пределами было совершено 8,2 млрд. операций на общую сумму 23,4 трлн рублей. В июне 2016 года эксперты сообщили о вероятности роста потерь от киберугроз во всем мире до $2 трлн. к 2018 году [24, стр. 42].

При этом количество вирусных атак в мире растёт со скоростью плюс 3% в месяц, атак на веб-сервисы - 2,5%, краж денежных средств с различных устройств или электронных кошельков - не менее 3,5%.

В России, по данным Сбербанка, потери от киберугроз составили 550-600 млрд. руб. в 2015 году, это примерно в 2 раза превышает ущерб от всех других экономических преступлений.

Он также привел данные ЦБ, что в прошлом году в России зафиксировано 32 тыс. попыток несанкционированных списаний у клиентов разных банков на общую сумму более 5 млрд. руб. Специалисты отметили 12-кратный рост количества инцидентов в этой области за последние 2 года.

За весь 2015 год Сбербанк зафиксировал 52 крупные хакерские атаки на свои системы, а с начала 2016 года ~ 57. В 2015-2016 годы все службы Сбербанка фиксируют рост различных централизованных атак на финансово-

кредитные учреждения РФ, в том числе на Сбербанк. Отмечено увеличение хакерских атак на все дистанционные банковские сервисы, которые предоставляются через интернет.

- Основным риском, который имеет прямые финансовые последствия, остается риск мошенничества.
- Риск влияет, как на клиентов подрывая доверие к дистанционным средствам обслуживания, так и на сами финансовые организации, которые стали нести прямые потери от атак на АРМ КБР.
- Плюс - Риск стать стоп фактором в развитии бизнеса и/или ИТ.

В ходе совместного расследования «Лаборатория Касперского», Европол и Интерпол обнародовали в феврале 2015 года беспрецедентную киберпреступную операцию, в рамках которой злоумышленники похитили 1 млрд. долларов США.

Киберограбление продолжалось два года и затронуло около 100 финансовых организаций по всему миру. Эксперты полагают, что за этим громким инцидентом стоит международная группировка киберпреступников из России, Украины, ряда других европейских стран, а также Китая.

Криминальная группировка, получившая название Carbanak, использовала методы, характерные для целевых атак. Однако в отличие от многих других инцидентов это ограбление знаменует собой новый этап: теперь киберпреступники могут красть деньги напрямую из банков, а не у пользователей. Деятельность киберпреступников из банды Carbanak затронула около 100 банков, платежных систем и других финансовых организаций из почти 30 стран, в частности из России, США, Германии, Китая, Украины, Канады, Гонконга, Тайваня, Румынии, Франции, Испании, Норвегии, Индии, Великобритании, Польши, Пакистана, Непала, Марокко, Исландии, Ирландии, Чехии, Швейцарии, Бразилии, Болгарии и Австралии. Как выяснили эксперты, наиболее крупные суммы денег похищались в процессе вторжения в банковскую сеть: за каждый такой рейд

киберпреступники крали до 10 миллионов долларов. В среднем ограбление одного банка — от заражения первого компьютера в корпоративной сети до кражи денег и сворачивания активностей — занимало у хакеров от двух до четырех месяцев.

Преступная схема начиналась с проникновения в компьютер одного из сотрудников организации посредством фишинговых приемов. После заражения машины вредоносным ПО злоумышленники получали доступ к внутренней сети банка, находили компьютеры администраторов систем денежных транзакций и разворачивали видеонаблюдение за их экранами. Таким образом, банда Carbanak знала каждую деталь в работе персонала банка и могла имитировать привычные действия сотрудников при переводе денег на мошеннические счета.

Эти ограбления банков отличаются от остальных тем, что киберпреступники применяли такие методы, которые позволяли им не зависеть от используемого в банке ПО, даже если оно было уникальным. Хакерам даже не пришлось взламывать банковские сервисы. Они просто проникали в корпоративную сеть и учились, как можно замаскировать мошеннические действия под легитимные.

Эти атаки служат очередным подтверждением того, что злоумышленники неизменно будут эксплуатировать любую уязвимость в любой системе. В таких условиях ни один сектор не может чувствовать себя в абсолютной безопасности, поэтому вопросам защиты стоит постоянно уделять внимание. Выявление новых тенденций в сфере киберпреступлений — одно из основных направлений, по которым Интерпол сотрудничает с «Лабораторией Касперского», и цель этого взаимодействия — помочь государственным и частным компаниям обеспечить лучшую защиту от этих постоянно меняющихся угроз».

Как происходила атака:

- В среднем ограбление одного банка — от заражения первого компьютера в корпоративной сети до кражи денег и сокрытия следов — занимало у хакеров от двух до четырех месяцев.
- Средняя сумма кражи ~10 000 000 USD.
- Заражение проходило или через письмо с вложением, как бы от сотрудника банка или клиента или через фишинг – по ссылке на WWW ресурс в который предлагалось ввести логин и пароль; сотрудники вводили свои логин и пароль в подложный сайт имитировавший корпоративный ресурс или систему.

Далее злоумышленники собирали информацию о процессе работы банка и находили удобный момент для совершения кражи, в том числе использовали для вывода средств S.W.I.F.T (который на первый взгляд кажется абсолютно защищенным) или системы дистанционного банковского обслуживания [66].


*Атака ANUNAK. Начало атаки Anunak – письмо с вредоносным вложением

Рис. 2.3. Схема операций атаки ANUNAK

Злоумышленниками использовано более 70 тыс.платежных карт, 70% из которых – расчетные (дебетовые). Всего в банкоматах, платежных терминалах, посредством Интернет-банка и мобильных приложений, уже в

2014 году мошенники похитили с банковских счетов граждан и компаний 3,5 млрд руб.

Наибольший объем несанкционированных операций зафиксирован на территории Москвы и Московской области, Центрального, Северо-Западного и Уральского федеральных округов. Интерес представляет график распределения операций по регионам по типу инфраструктуры. Если в среднем по регионам мошенники отдают примерно равное предпочтение Интернету (стационарному и мобильному) и банкоматам, то в Северо-Кавказском округе доля несанкционированных операций в Интернете достигла 81%. А самое большое число попыток мошенничества в пунктах выдачи наличности (10%) зафиксировано в Крыму.

Для выуживания персональных данных держателей карт и их кредиток (фишинга) мошенники активно используют методы социальной инженерии (науки об управлении поведением человека без технических средств, на основе психологии). Стандартная фишинговая схема начинается с SMS о блокировке карты. Доверчивые люди звонят по телефону, указанному в SMS и называют «сотрудникам службы безопасности банка» номер карты для проверки, CVV-код и другие данные. Если карта жертвы защищена системой 3D Secure, для завершения транзакции нужен пароль, который автоматически поступает на телефон. Поэтому мошенники говорят, что для разблокирования карты пришлют проверочное SMS-сообщение и клиент должен назвать код, указанный в нем. На самом деле в этот момент они совершают покупку через интернет-магазин либо переводят средства на свою карту или счет мобильного телефона.

Мошенники могут представиться сотрудниками службы безопасности или контактного центра банка и убедить клиента - подойти к ближайшему банкомату, выполнить под их контролем операции по «спасению» средств. Следуя инструкциям по телефону граждане собственными руками переводят

средства на электронные кошельки, банковские карты или телефоны мошенников.

Растет количество обманутых клиентов банков, которых завлекли на подложные интернет-сайты с очень низкими ценами на авиабилеты или бытовую технику. В опцию оплаты на поддельном сайте мошенники «встраивают» сервисы перевода денег с карты на карту с вводом одноразового пароля, который приходит по SMS. Клиент опрометчиво вводит пароль, будучи уверенным в оплате покупки. При этом в SMS указывается - на какие цели идут средства: если видно, что это перевод на карту, а клиент совершает покупку, он ни в коем случае не должен вбивать и передавать кому-либо этот код [65].


Рис. 2.4. Статистика структуры угроз на 2017 год

Наибольшее число несанкционированных операций выполнено в процессе переводов денежных средств на территории РФ (доля внутрироссийских несанкционированных операций составила 47% от объема и 41% от количества всех несанкционированных операций). Чаще всего мошенники использовали реквизиты реальных банковских карт (от 65% до

72%, в зависимости от квартала), затем — поддельный «пластик» (от 18% до 24%), и 10-11% — данные утерянных или украденных карт.

Популярным видом мошенничества скимминг (кража данных карты при помощи считывающего устройства на банкоматах и других платежных устройствах общего пользования).

Чтобы уберечься от этого вида жульничества, не надо пользоваться банкоматами в плохо освещенных и безлюдных местах. Нужно использовать банкоматы надежных и проверенных банков, не допускать сторонних наблюдателей при снятии наличных, не прибегать к помощи посторонних лиц.

Банкиры просят клиентов внимательно осмотреть банкомат, прежде чем ввести ПИН-код. Вводя пин-код, всегда прикрывайте клавиатуру. Это не позволит мошенникам увидеть пин-код или записать его на видеокамеру. Памятка по безопасности условий использования карт Сбербанка, например, является частью договора и клиент обязан соблюдать установленные в ней правила. Если банк докажет запись пин-кода мошенниками при помощи видеокамеры потому, что клиент не прикрыл клавиатуру рукой, суд вполне может и отказать клиенту в возмещении украденного.

Риски, связанные с использованием ДБО разделяют на те, которые возникают на стороне клиента, и те, что характерны для финансово-кредитных организаций. При этом Сергей Котов подчеркивает, что такие риски специфическими считать не следует, поскольку они актуальны не только для области ДБО.

Для клиентов ДБО характерны кражи и потери средств, применяемых для идентификации пользователей (в том числе ключей формирования электронных подписей платежных поручений), перехват управления вычислительными ресурсами как стационарных, так и мобильных устройств, применяемых для работы с сервисами ДБО, заражение их вредоносными программами, позволяющими нарушать целостность последовательности

действий при формировании платежных поручений. Эксперты указывают на то, что ситуация с обеспечением безопасности использования систем ДБО на стороне клиентов усложняется их низкой ИБ-культурой.

Отчет Cisco по информационной безопасности за первое полугодие 2017 года указывает на быструю эволюцию угроз и рост их масштабов, а также на распространение атак типа «прерывание обслуживания» (destruction of service, DeOS), которые способны уничтожать резервные копии и страховочные системы (safety net), необходимые организациям для восстановления систем и данных после атаки. С появлением интернета вещей (Internet of Things, IoT) все больше операций в ключевых отраслях переводится в онлайн-режим, что расширяет горизонт атак, увеличивает их масштабы и усугубляет последствия [63].

Недавние атаки WannaCry и NotPetya продемонстрировали скорость распространения вредоносного ПО, которое выглядит как программа-вымогатель, но на самом деле способно вызвать куда более существенные разрушения в информационно-технологической сфере. Это предвещает появление угроз, которые Cisco назвала атаками типа «прерывание обслуживания»: они чрезвычайно опасны потому, что в случае успешного их проведения пострадавший бизнес фактически полностью лишается возможности восстановиться [68].

Впрочем, есть и другие очень опасные явления в сфере ИБ: самыми опасными считает «тихие» атаки, которые могут долгое время оставаться незамеченными. Цель атак может быть различной – похищение данных, финансовые хищения, проникновение к партнерам, эксплуатация ресурсов или все эти цели сразу. Были зафиксированы прецеденты, когда злоумышленники годами использовали инфраструктуру банковской организации, и сотрудники, отвечающие за обеспечение информационной защиты компаний, даже не догадывались об этом – естественно, до того момента, когда ущерб бизнесу становился реальным и очевидным.

На стороне кредитно-финансовых организаций отметим недостаточный контроль используемых бизнес-процессов, низкую эффективность взаимодействия банков между собой и с правоохранительными органами, уязвимости в базовом ПО систем ДБО, злонамеренный инсайд со стороны банковских сотрудников, включая администраторов бизнес-приложений и инфраструктуры.

Нами обобщены исследования «Лаборатории Касперского», основное это прямые потери финансовых организаций от кибератак. Помимо прямого ущерба это дополнительные расходы на заработную плату персонала, привлечение внешних специалистов, репутационные издержки, упущенную выгоду, а также страховые выплаты и компенсации клиентам.

Предложены основные этапы информационной безопасности (рис. 2.5):

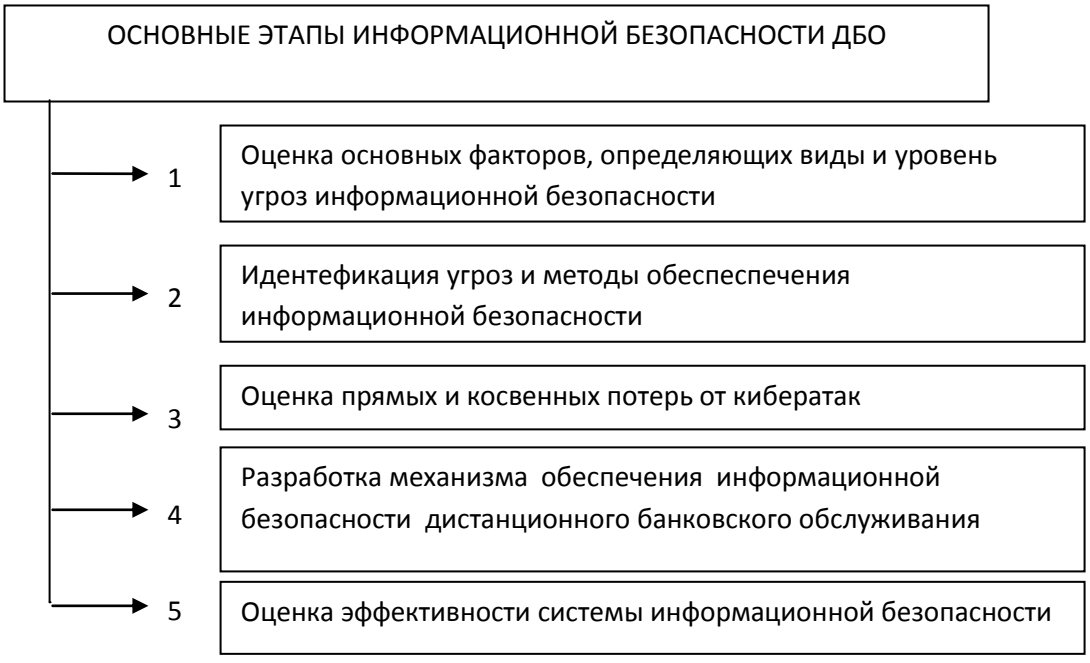


Рис. 2.5. Основные этапы формирования системы информационной безопасности коммерческого банка

Эксперты «Лаборатории Касперского» при разработке стратегии кибербезопасности советуют принимать во внимание также следующие рекомендации:

- необходимо остерегаться целевых атак. Они могут проводиться через третьих лиц или ваших подрядчиков. Такие компании часто слабо защищены, что может стать вашей проблемой;
- надо учитывать человеческий фактор: злоумышленники очень часто и изобретательно применяют методы социальной инженерии для проникновения в инфраструктуру компании;
- помнить, что одно лишь соответствие требованиям безопасности не дает гарантированной защиты. Не менее важно применять комплексный подход к безопасности;
- проводить регулярные тесты на проникновение. Уязвимости инфраструктуры должны быть известны вам раньше, чем до них доберутся злоумышленники.
- Принимать во внимание угрозу инсайдеров. Злоумышленники могут подкупить сотрудников компании, чтобы обойти систему защиты. Противостоять этому можно применением политик ИБ, грамотным разграничением доступа и вспомогательными методами для обнаружения аномальных активностей внутри организации.

## 2.4. Стратегические направления обеспечения информационной безопасности

Характерной особенностью современной мировой экономики выступает переход на новый технологический уклад. На данном этапе точкой роста становится стремительное развитие информационных технологий. Мы наблюдаем за успехами и достижениями человечества в области развитий

технике. Современная техника внедряется в производство и в общественную жизнь человека. Нетрудно заметить, что цифровые технологии и программные обеспечения положительно воздействуют на дальнейшее развитие и на повышение доходности компаний.

Цифровая экономика стала базой развития и оказывает воздействие на такие отрасли как: банковская, розничная торговля, транспорт, энергетика, образование, здравоохранение и многие другие. Цифровые технологии, такие как интернет, мобильные устройства, преобразуют способы социального взаимодействия и влияют на экономические отношения.

Цифровая экономика - экономическая деятельность, которая построена на цифровой технологии. В России цифровая экономика находится на стадии развития. Важным аспектом продвижения цифровой экономики в России является обеспечение информационной и экономической безопасности государства, а так же защиты важных данных и неприкосновенности российских граждан в цифровом пространстве.

Цифровая экономика – это современное развитие, основанное на использовании электронных систем, которая предлагает обмен данных между участниками процессов в режиме онлайн. Преимуществом цифровой экономике является:

- упрощение взаимодействий деловых сторон, делая управление экономическими процессами более простым;

- легко входят в существующие процессы, которые протекают в государстве.

Цифровая экономика формирует новые бизнес-модели. Поэтому компаниям, необходимо знать, как использовать новшества этих бизнес-моделей. Современное цифровое развитие техники потребуют радикальных изменений в компаниях. Это влечет за собой необходимость подготовки качественно новых сотрудников. В России уже существует курс "Цифровая трансформация", и данное обучение на сегодняшний день необходима

практически каждому современному специалисту в любой отрасли и сфере деятельности.

Планируется с 2019 года в Российских школах обучать основам цифровой экономики школьников. К внедрению в школьную программу предлагается предмет «Технология», вести который будут специалисты-практики. Современное поколение получит возможность получить профессиональную подготовку в ИТ-сфере, что позволит избежать безработицы, связанной с «вытеснением» людей техническими роботами.

Продвижение цифровой экономики требует усилий, как от бизнеса, так и со стороны государства. Цифровая экономика становиться не просто продвижением в науке информационных технологий, но и вносит большие изменения в бизнес-модели. Поэтому на данный момент необходимо развивать электронные сервисы в государственном секторе и внедрять цифровые технические новшества на уровне отдельно взятой компании. Успех развития цифровой экономики зависит от того, как государственный, и корпоративный сектор будут двигаться в сторону цифрового развития.

Цифровая экономика невозможна без участия государства. Коммерческие компании, понимая выгоду, сами запускают процессы собственной цифроризации, а вот с государственными ведомствами дело обстоит несколько сложнее, так как здесь необходима инициатива государства, изменение законодательства, и на решение таких вопросов может потребоваться не один год [56].

Цифровая экономика - это не отдельная отрасль, по сути это уклад жизни, новая основа для развития системы государственного управления, экономики, бизнеса, социальной сферы, всего общества. Конечно, формирование цифровой экономики - вопрос национальной безопасности и независимости России [52].

Цифровая экономика стала одним из главных направлений развития РФ до 2025 года. Корпорации уже начали формировать департаменты по

развитию цифровой трансформации, но столкнулись с нехваткой специалистов по данному направлению. 31 июля 2017 года была утверждена Программа "Цифровая экономика". Цель программы - организовать системное развитие и внедрение цифровых технологий во всех областях жизни - и в экономике, и в предпринимательстве, как социальной деятельности и в государственном управлении, социальной сфере и в городском хозяйстве. Перевод экономики в цифру - вопрос нашей глобальной конкурентоспособности и национальной безопасности. Горизонт исполнения программы 2025 год [55].

Россия взяла курс на развитие цифровой экономики, ведя страну к новому уровню жизни. И в ближайшие десятилетия все отрасли и рынки, будут стремиться перестроиться на современный лад с требованиями новых цифровых моделей.

Цифровая экономика вступила в силу развития по всему миру. У современного научного технологического прогресса большинство выделяют положительные стороны, но смотря в будущее, данная разработка имеет и минусы, к примеру, киберугрозы. Проблема России — в огромном количестве подходов, взглядов, недооценке рисков. А существенных изменений в области взаимодействия государства и бизнеса по этому вопросу нет. У нас недостаточно мер право применения и прав охранения, чтобы противодействовать угрозе. Нужна следующая схема: компании создают собственные центры противодействия киберугрозам, они потом превращаются в фьюжн-центры, а те в свою очередь смогут управлять инцидентами. Результаты работы переходят к государственным институтам, после чего разрабатывается право применение [54].

Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления [53].

Цифровая экономика – это научный прорыв, который несет упрощение работ во многих сферах, но не стоит забывать, что впереди нас может ожидать угроза массовых безработиц после внедрения цифровых технологий.


Рис. 2.6. Рекомендации по адаптации зарубежного опыта при разработке банковских продуктов, услуг и их безопасности

«Сбербанк» в сотрудничестве с Федеральной службой безопасности (ФСБ) разрабатывает общероссийскую систему защиты от

киберпреступников. Ей смогут воспользоваться и другие банки. Система будет разработана к 2018 году. Сейчас у «Сбербанка» есть центры кибербезопаности в пяти городах, где работают около тысячи специалистов, которые ежедневно регистрируют около 1 млн. инцидентов. По словам топ-менеджера банка, в первой половине 2016 года они смогли предотвратить кражи средств на 8 млрд. рублей. Системой смогут воспользоваться и другие российские банки, которые обращаются к «Сбербанку» за помощью в случае кибератаки.

«Сбербанк» не просит плату за помощь, но после разработки системы это может измениться. Разрабатываемая банком платформа будет платной для других кредитных организаций. Предполагается, что в основу системы лягут разработки дочерней компании «Сбербанка» «Бизон», которая специализируется на выявлений нарушений прав финансово-кредитных организаций и тестировании систем кибербезопасности банка. Новая платформа может стать конкурентом для «Лаборатории Касперского» — единственной российской компании, специализирующейся на кибербезопасности, которая известна во всём мире.

При этом, не все банки будут готовы предоставить «Сбербанку» свои данные, опасаясь утечки клиентов. В то же время они признают необходимость сотрудничества в борьбе с кибератаками, которые становятся всё опаснее. Будет лучше, если управление [системой] возьмёт на себя третья сторона, чтобы избежать конфликта интересов. Регулятор Центробанк — это наиболее подходящий посредник.

Ежегодно на защиту от кибератак «Сбербанк» тратит 1,5 млрд. рублей (около $23,4 млн). Для сравнения: расходы на защиту от киберпреступников американского банка JPMorgan Chase составляют $600 млн. в год.

Среди многочисленных проблем обеспечения информационной безопасности поднимается тема противодействия современным киберугрозам в финансово-банковском секторе и способы противодействия, требования к

кадрам, в том числе необходимость повышения общего уровня киберграмотности сотрудников компаний и госслужащих.

По результатам исследования Аналитического центра InfoWatch в России в 2016 году был зафиксирован рост количества утечек информации на 80 % по сравнению с 2015 годом. При этом в девяти из десяти случаев утекали персональные данные (ПДн) и платежная информация.

Неготовность российской судебной системы к работе с цифровыми доказательствами несовершенна. Судебная система фундаментально не готова рассматривать цифровые доказательства киберпреступлений в качестве аргументов ни в арбитражном, ни в уголовном процессе. Необходима законодательная основа, которая позволит применять более жесткие меры в отношении киберпреступников, и экосистема кибербезопасности, подключение к которой обеспечит защищенность от киберугроз. При этом, 80% успеха при обеспечении кибербезопасности зависит от того, насколько правильно выстроены процессы, и только 20% – от технологий. Безопасность должна прежде всего закладываться в процессах и только потом начинают эффективно работать технологии, инструменты и ИБ-команда.

Кибербезопасность в большей степени зависит от правильно выстроенных процессов. Большинство игроков на рынке используют одинаковые или схожие технологии безопасности, но даже с одинаковыми технологиями одна компания может пострадать от кибератаки, а другая – нет. И не пострадает та компания, которая корректно произвела настройки, поставила обновления на ПО, вовремя обнаружила атаку и среагировала на нее, а это уже операционная составляющая. Все вышесказанное справедливо только при условии наличия ресурсов. Если же присутствует значительная недофинансированность или не хватает иных, нефинансовых ресурсов для обеспечения ИБ компании, тогда без должного технологического

инструментария процессы будут очень громоздкими и трудоемкими, а значит, неэффективными.

Именно отлаженность процессов является главным компонентом кибербезопасности. Если система изначально настроена правильно, алгоритм работы понятен всем участникам, то уровень защиты может быть очень высоким. Безусловно, новые технологические решения также существенно помогают повысить уровень эффективности работы, но это инструмент, который должен быть в надежных руках.

Именно проблема квалифицированных кадров по-прежнему является одной из самых насущных. Она имеет особую актуальность на протяжении всех последних лет, потому что на сегодняшний день человек остается самым уязвимым звеном в ИТ-инфраструктуре.

Самое слабое звено в информационной безопасности банка – это сотрудник компании. Если сотрудники не соблюдают правила безопасности, то технологии не смогут помочь защититься. При использовании социальной инженерии злоумышленники могут заставить сотрудника организации совершить какое-то действие, которое упростит проведение атаки. Часто, чтобы подобрать пароль к аккаунту, злоумышленнику не обязательно его взламывать – вся информация о пароле есть в профилях социальных сетей или рядом с рабочим столом. Даже сотрудники на руководящих позициях производят манипуляции, спровоцированные злоумышленниками. Отдельно можно отметить нежелание сотрудников следовать политикам и требованиям по ИБ, потому что это может усложнить их работу. В результате они игнорируют риски, которые таким образом появляются.

Чтобы минимизировать влияние человеческого фактора, нужно постоянно повышать осведомленность сотрудников в области информационной безопасности, а также внедрять систему контроля и мониторинга соблюдения политик и требований в области ИБ.

Среди основных способов минимизации угрозы ИБ выделяют повышение осведомленности персонала в вопросах информационной безопасности, проведение тестов, деловых игр, киберучений.

Наряду с человеческим фактором серьезную угрозу для информационной безопасности компании представляют устаревший парк оборудования и не поддерживаемое производителем ПО, отсутствие решений для мониторинга корпоративной сети, утечка баз данных через сотрудников, ИТ-аутсорсеров, разработчиков ПО.

В связи с проблемой рисков, которые несет человеческий фактор, любопытно вспомнить исследование антивирусной компании ESET, опубликованное в июле 2017 года. Четыре компании из пяти недооценивают риски информационной безопасности, связанные с человеческим фактором. Такой вывод сделали сотрудники ESET после опроса интернет-пользователей из России и СНГ. Респондентам предложили выбрать ответ на вопрос: «Проходили ли вы на работе тренинг по информационной безопасности?». Поразительный для нашего времени факт, но результат был следующим: отрицательный ответ лидирует с большим отрывом. 69 % респондентов никогда не проходили обучение основам кибербезопасности в своих компаниях. Еще 15 % участников опроса сообщили, что их работодатели ограничились минимальным объемом информации. Обучение не выходило за рамки «в случае неполадок перезагрузите компьютер», правила кибербезопасности не затрагивались.

Только 16% респондентов прошли качественные тренинги с подробным рассказом об информационной безопасности и актуальных угрозах.

Для сравнения: больше 60% участников аналогичного опроса в США сообщили, что их работодатели организовали для них обучение по кибербезопасности.

Далее участникам опроса ESET предложили перечислить аспекты компьютерной безопасности, информации о которых им не хватает для обеспечения защиты. Респонденты честно признали наличие пробелов в своих познаниях.

70 % участников сообщили, что недостаточно знакомы с темой безопасности беспроводных сетей, в частности угрозами для Wi-Fi.

Вторую строку рейтинга пробелов в знаниях занимают программы-вымогатели. 63% респондентов считают, что им недостает знаний для защиты от шифраторов.

Другие категории вредоносного ПО – банковские трояны и вредоносные программы для мобильных устройств – получили по 56% голосов. 57% участников опроса хотели бы знать больше о безопасности паролей, 51% – о защите от «классических» инструментов интернет-мошенников (фишинга и спама).

Как показали исследования, большая часть нарушений информационной безопасности в компаниях связана с ошибками персонала. На человеческом факторе – социальной инженерии – и старых уязвимостях ПО построены целевые атаки на организации. Снизить риски и найти слабое звено в компании раньше, чем это сделают злоумышленники, позволяет обучение сотрудников, а также разного рода тесты, определяющие внутренние угрозы безопасности.

Эксперты отмечают, что скорость изменения и появления новых технологий стала причиной кадрового голода, а в среде специалистов по ИБ по всему миру наблюдается нулевая безработица. Проблему нехватки кадров в сфере информационной безопасности для финансовой индустрии на сегодня выделяют в основную. Работа современной финансовой системы невозможна без применения принципа security by design (разработка информационных систем, изначально защищенных от различного рода угроз), для чего нужны квалифицированные специалисты.

Кадровая проблема вызывает необходимость появления новых профессий на стыке ИТ и других дисциплин. Например, требуется совмещение профессии специалиста по безопасности и юриста. Такие специалисты могли бы помочь правоохранительным органам в борьбе с киберпреступниками.

Кибербезопасность – одна из самых динамично развивающихся отраслей, поэтому спрос на кадры очень высокий. А образовательный рынок отреагировать на эту тенденцию успел не в полной мере, именно с этим связана данная проблема. Но через 3-5 лет ситуация с кадрами будет значительно лучше. Приходится довольно долго искать нужных людей, как правило, с опытом, с необходимой квалификацией. Требования к квалификации, опыту и компетенциям специалистов диктуются сложностью и многообразием применяемого для защиты информации оборудования и ПО. Ведь, несмотря на помощь интегратора или вендора при внедрении средств защиты, дальнейшая эксплуатация решения лежит на плечах ИБ-команды компании. Именно поэтому наиболее опасны те атаки, которые организованы профессионалами, имеющими опыт работы в индустрии ИБ. Например, если речь идет о каких-то спланированных атаках в интересах крупных групп влияния. В этом случае уровень опасности очень высокий.

Любая нештатная ситуация – это проверка на профпригодность безопасников, айшников. Последние события с атаками WannaCry, NotPetya и др. это наглядно показали. Самыми эффективными атаками для средних и малых компаний являются довольно примитивные и понятные в реализации виды атак, такие как попытки вторжения через уязвимости в ПО, обман или злоупотребление доверием, заражение вредоносным ПО через фишинговые рассылки по каналам электронной почты, целевые атаки на персонал с необходимым уровнем доступа.

Большинство из таких атак можно было бы предотвратить, применяя базовые принципы защиты информации, которые предложены специалистами банка «Глобэкс» и нами сгруппированы (рис.2.7).

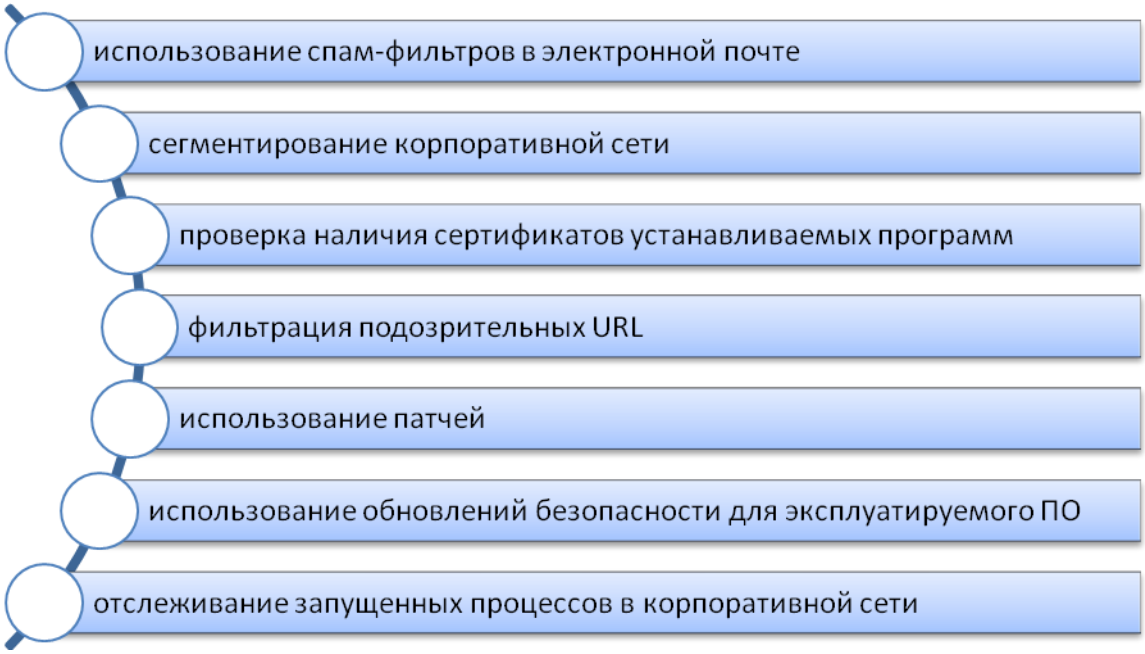


Рис.2.7. Базовые принципы защиты информации банка «Глобэкс»

Наряду с этим важно осуществлять сканирование антивирусными решениями (обновление антивирусных баз), настройку поведенческого анализа в антивирусных решениях, использовать файрвол, межсетевые экраны. Конечно, работники компании не должны открывать ссылки в письмах, пришедших из непроверенных источников. Наконец, необходима организация обмена информацией об инцидентах между участниками информационного взаимодействия в рамках центров реагирования на компьютерные преступления.

Наиболее актуальные угрозы информационной безопасности банков в последнее время связаны с целенаправленными атаками: на адреса сотрудников рассылаются почтовые сообщения, содержащие вредоносное ПО. Также актуальными остаются угрозы, связанные с DDoS-атаками и

атаками на клиентов систем дистанционного банковского обслуживания (ДБО).

Минимизировать такие риски можно путем внедрения современных систем защиты и эффективных процедур реагирования, выполнения требований информационной безопасности, повышения осведомленности персонала в области информационной безопасности и реализация других мероприятий (рис.2.8).

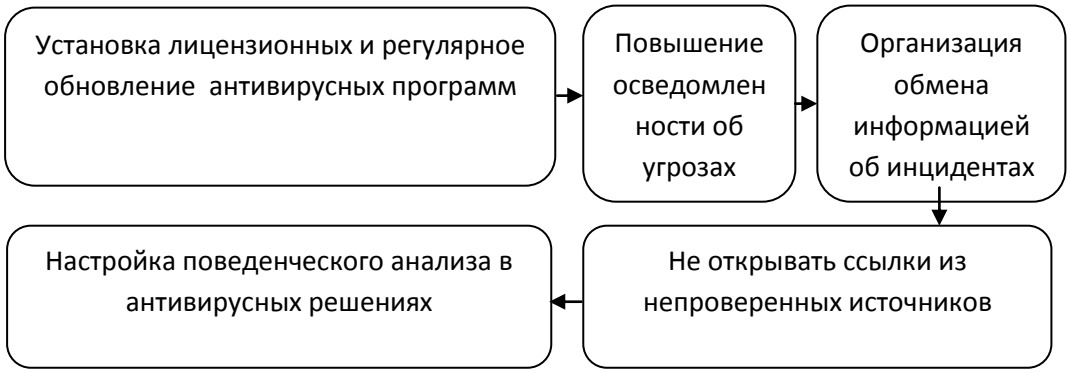


Рис. 2.8. План мероприятий обеспечения информационной безопасности

Так же при разработке мобильных приложений необходимо анализировать и пресекать уязвимости и угрозы в области безопасности. На регулярной основе проводить проверки уязвимости приложений с привлечением внешних специализированных компаний. Внешний подрядчик с надежной репутацией и опытом работы на рынке будет обладать большей компетенцией, в том числе компетенцией по части безопасной разработки.

К примеру, в ВТБ 24 внедрена антифрод-система, которая выявляет аномальное поведение клиентов в дистанционном банковском обслуживании (ДБО) и останавливает мошеннические операции. В приложениях ВТБ 24 многофакторная аутентификация работает во всех системах ДБО. В мобильном приложении ВТБ 24 не зафиксировано ни одного случая взлома.

В последнее время крупные банки запустили у себя пилотные проекты по использованию средств биометрической идентификации. Конечно, пока

еще остается слишком много вопросов в этой сфере. Трудно определить, какой из видов биометрии наиболее эффективен и применим на практике, как подойти к внедрению биометрии с технологической точки зрения, а также с точки зрения правового и методологического обеспечения самого процесса идентификации клиентов по биометрическим данным. Ведь перспективы использования биометрических технологий до сих пор сдерживаются пробелами в действующем законодательстве, высокой стоимостью и несовершенством решений. Однако при всем при этом крупные финансово-кредитные институты уже сегодня используют биометрические технологии в целях обеспечения информационной безопасности, противодействия внешнему и внутреннему мошенничеству. Например, банку ВТБ 24 интересна возможность применения биометрических технологий, прокомментировали в пресс-службе организации. «Преимущество биометрии – удобство клиента. Пароли могут быть потеряны или украдены, а биометрические данные уникальны, поэтому можно говорить о надежности метода», – считают специалисты ВТБ 24.

В начале 2017 года ВТБ 24 завершил пилотный проект по голосовой идентификации клиентов при обращении в контактный центр, что позволяет создать удобный для клиента и достоверный для банка процесс подтверждения операций. Это может в разы увеличить объем проверяемых операций и минимизировать риски клиентов и банка, считают в финансово-кредитной организации. Также ВТБ 24 запустил проект биометрической аутентификации клиентов по внешности в новом типе офисов с безбумажным обслуживанием. При посещении таких отделений клиенты подписывают только электронные версии документов. При этом, помимо традиционной идентификации по паспорту, банк предлагает пройти аутентификацию на планшете, которая дополнительно подтверждает, что именно этот человек в определенный день и время подписал документы.

В розничном бизнесе банка ВТБ и ВТБ 24 уже внедрен сервис использования отпечатка пальца в мобильном банке на вход, а в розничном бизнесе банка ВТБ – еще и на подтверждение операций.

Исследовав теорию и практику обеспечения информационной безопасности, нами выделены основные подходы и характерные признаки становления системы ИБ поэтапно (рис. 2.9).

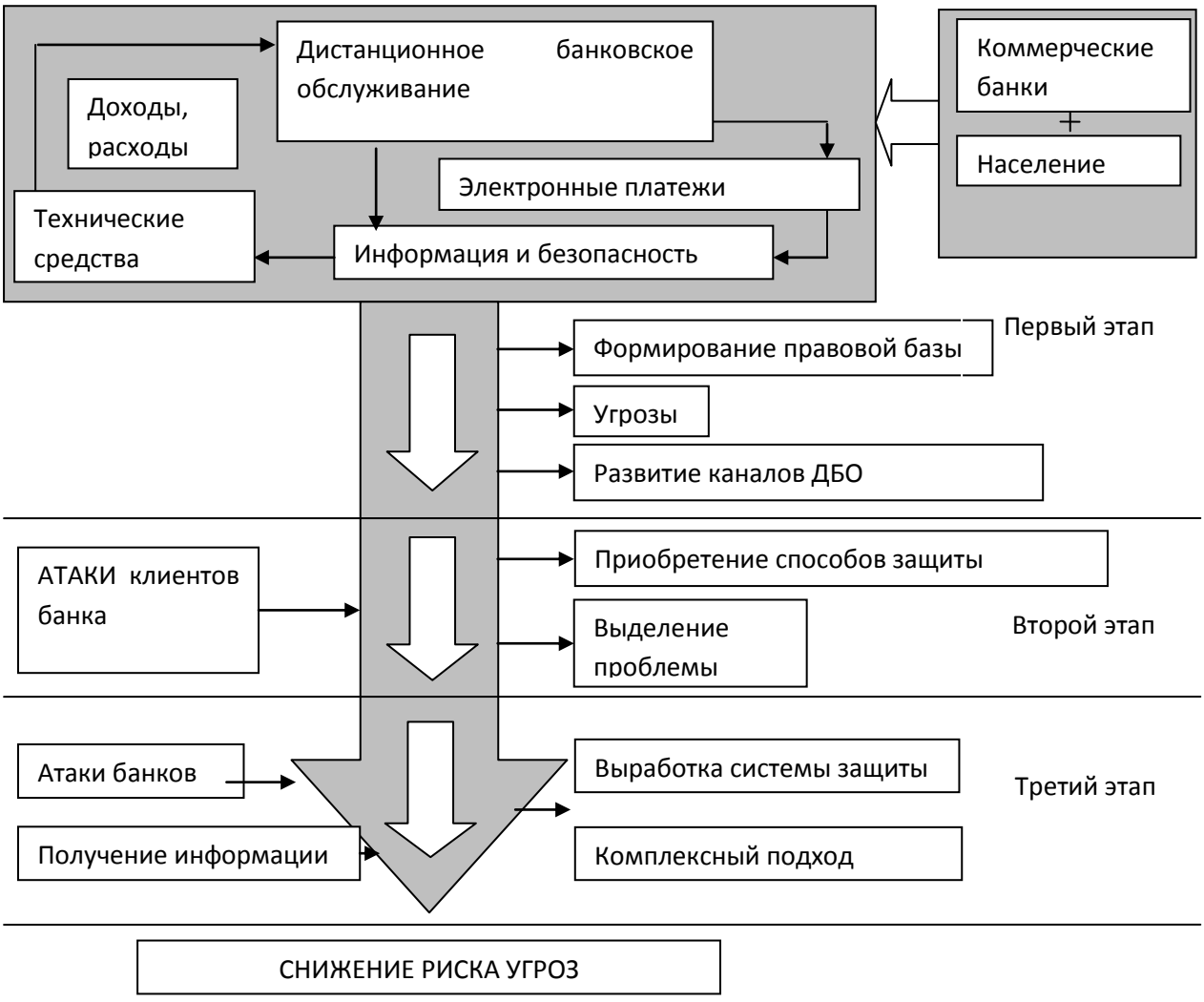


Рис. 2.9. Формирование системы информационной безопасности

Самым значимым в области регулирования ДБО в России является принятый 27 июня 2011 года федеральный закон № 161-ФЗ “О национальной платежной системе”. Его появление свидетельствует о серьезных намерениях государства в регулировании функционирования платежных систем, и одним

из результатов создания национальной платежной системы станет повышение общей защищенности систем ДБО. Разработка и корректировка закона проходит в тесном контакте госрегуляторов, производителей средств ИБ и специалистов служб безопасности банков.

Так, Банк России уже ведет разработку специализированных нормативных документов по информационной защите, среди которых можно назвать стандарт Банка Росси СТО БР ИББС и Положение Банка России 382-П от 9 июня 2012 г. о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке контроля со стороны Банка России за соблюдением этих требований.

Наиболее сложным и опасным на сегодняшний день атакам на ДБО в результате которых происходит подмена платежных документов на этапе их подписания. Во время такой атаки пользователь видит и подписывает один документ, а в банк уходит подложный. Вредоносные программы, лежащие в основе организации таких атак, хакерами разработаны практически для всех наиболее распространенных систем ДБО, а ущерб от этого типа атак сегодня исчисляется десятками миллионов рублей.

Таким образом, можно оценить состояние регулирования и контроля исполнения требований регуляторов в сфере ДБО нашей страны как зачаточное. Выдвинутые в законе “О национальной платежной системе” требования являются необходимыми для регулирования обращения платежей в стране. Вместе с тем закон получил ряд серьезных замечаний со стороны банковского сообщества, которые повлекли за собой необходимость его корректировки и уточнений. По мере развития финансовых технологий и их инкорпорирования в банковский бизнес будут возрастать и риски в сфере ИБ, и требования к профильным управлениям и департаментам, что вызвано комплексным подходом в решении этой актуальнейшей проблемы.

# ЗАКЛЮЧЕНИЕ

Дистанционное банковское обслуживание (ДБО) - неотъемлемая часть банковских услуг клиенту с использованием телефонных и компьютерных сетей, без его непосредственного визита в банк. Это инструмент снижения операционных расходов, повышения эффективности и конкурентоспособности бизнеса банков. В настоящее время отмечается стабильный рост уровня распространенности ДБО: такие системы используют 94% российских банков. Согласно данным Банка России доступом к своим банковским счетам пользуется несколько миллионов физических лиц. Распространение ДБО особенно активно происходило в периоды кризисов, наряду со стремлением руководителей банков сократить свои издержки путем внедрения сравнительно доступной формы обслуживания. Вместе с тем недостаточное внимание, уделяемое проблемам информационной безопасности и защиты информации, привело к целому ряду уязвимостей, хорошо известных в сфере безопасности приложений, а также угрозам, связанным со спецификой банковской сферы, реализация которых может привести к существенным финансовым и репутационным потерям.

Информационная безопасность и риски в системы ДБО связаны с динамичным ростом этого сегмента рынка. Около 70% систем ДБО являются собственными разработками банков. В ходе анализа защищенности систем ДБО за 2017 год было выявлено, что во всех системах имеются свои слабые стороны. В общей сложности было выявлено свыше 170 уязвимостей, большинство из которых определяются низкой степенью риска. Это говорит о том, что в сравнении с результатами предыдущих годов общая доля критически опасных уязвимостей в 2017 году заметно снизилась. МВД России сообщает, что растут как количество, так и размеры хищений

денежных средств индивидуальных и корпоративных вкладчиков, осуществляемых с использованием ДБО. При этом денег у юридических лиц крадётся в тысячи раз больше, чем у физических. Вместе с этим, по сравнению с постоянно растущим объемом возможных угроз, уровень защищенности систем ДБО в целом значительно отстает. При этом количество вирусных атак в мире растёт со скоростью плюс 3% в месяц, атак на веб-сервисы - 2,5%, краж денежных средств с различных устройств или электронных кошельков - не менее 3,5%.

По сравнению с 2015-2016 гг., в 2017 году количество серьезных угроз дистанционного обслуживания банков увеличилось на 12% и достигло 90%, что говорит о необходимости принятия необходимых мер, для создания условий полной защищенности.

В России, по данным Сбербанка, потери от киберугроз составили 550-600 млрд. руб. в 2015 году, это примерно в 2 раза превышает ущерб от всех других экономических преступлений.

Он также привел данные ЦБ, что в прошлом году в России зафиксировано 32 тыс. попыток несанкционированных списаний у клиентов разных банков на общую сумму более 5 млрд. руб. Специалисты отметили 12-кратный рост количества инцидентов в этой области за последние 2 года.

За весь 2015 год Сбербанк зафиксировал 52 крупные хакерские атаки на свои системы, а с начала 2016 года ~ 57. В 2015-2016 годы все службы Сбербанка фиксируют рост различных централизованных атак на финансово-кредитные учреждения РФ, в том числе на Сбербанк. Отмечено увеличение хакерских атак на все дистанционные банковские сервисы, которые предоставляются через интернет.

Ежегодно на защиту от кибератак «Сбербанк» тратит 1,5 млрд. рублей (около $23,4 млн). Для сравнения: расходы на защиту от киберпреступников американского банка JPMorgan Chase составляют $600 млн. в год., в 25,7 раза больше.

Сбербанк стремится сделать технологические инновации частью собственной ДНК, научиться встраивать их в существующие бизнес-процессы, запускать на их основе новые бизнес-модели.

Технологические инновации позволят сделать ИТ-системы, инфраструктуру и процессы Группы:

— надежными - через обеспечение высокого уровня надежности и доступности всех ИТ-услуг и за счет упрощения архитектуры, централизации и модернизации инфраструктуры;

— гибкими – через обеспечение максимальной скорости вывода продуктов на рынок, увеличение масштабируемости ИТ-систем, упрощение и стандартизацию архитектуры, технологий и процессов;

— эффективными по затратам – благодаря максимальной оптимизации затрат на ИТ и общих расходов бизнеса Сбербанка;

— соответствующими требованиям будущего – благодаря формированию прочного технологического фундамента для дальнейшего развития банка на срок, превышающий действие новой Стратегии.

Модернизация технологической платформы:

— информационные системы Сбербанка позволяют выдерживать рост транзакционной нагрузки на 40–45 % и пиковой нагрузки на основные системы в среднем на 70 % в год;

— полностью реализована программа централизации ИТ-систем; сегодня Сбербанк строит принципиально новую технологическую платформу, не имеющую аналогов в мире.

Надежность:

— доступность критичных систем Сбербанка составляет 99,99 %;

— более чем в 10 раз снижено время технологических простоев: в 2012 году – 800 часов, в 2016 году – 74 часа;

— почти в 20 раз снижено время простоев из-за инцидентов: в 2012 году – 1056 часов, в 2016 году – 54 часа;

— ЦОД «Южный Порт», введенный в эксплуатацию в 2012 году, сертифицирован по общепризнанным стандартам Tier III и Tier Sustainability GOLD;

— в 2016 году началось строительство ЦОД в инновационном центре «Сколково», который станет крупнейшим в Российской Федерации и одним из крупнейших в Европе. Банк меняет подход в управлении IT-инфраструктурой от принципа доступности ИТ-систем к качеству и надежности бизнес-сервисов.

Гибкость:

— существенно повысилась скорость запуска новых проектов с ИТ-составляющей: с 7 проектов в 2011 году до 270 – в 2016 году.

Эффективность проектов:

— Сбербанк превосходит ведущие мировые банки по ключевым показателям эффективности ИТ (ИТ-расходы, численность и затраты на ИТ-персонал);

— на фоне роста нагрузки стоимость операции неуклонно сокращается.

Операционная модель:

— Сбербанк снизил численность сотрудников, занимающихся сопровождением клиентских операций, с 58 тыс. человек в 2008 году и до 10 тыс. – 2016 году;

— процессы ИТ-сопровождения Сбербанка сертифицированы по CMMI (Level 3);

— проводится Agile-трансформация банка, которая заключается в переходе на метод гибкой разработки («Sbergile»). По ее окончании будут обеспечены максимальная гибкость разработки и максимальная скорость вывода продуктов на рынок.

Супермассивы данных:

— сегодня Сбербанк обрабатывает петабайты (1015) данных;

— анализ больших данных по активности клиентов позволил снизить уровень неработающих кредитов, сократить риски, что, в свою очередь, привело к снижению процентных ставок по кредитам, формированию специальных предложений с более интересными условиями для разных сегментов заемщиков.

Инновации:

— основная стратегическая инновация Сбербанка – создание новой технологической платформы и реализация сервисов на ее основе;

— Сбербанк постоянно исследует появляющиеся технологии с точки зрения возможности их применения и потенциальной пользы;

— основные направления прорывных инноваций в 2016–2017 годах: блокчейн, интернет вещей, машинное обучение, биометрия, облачные вычисления;

— Сбербанк активно вовлекает сотрудников в работу с текущими инновациями: в 2016 году задействовано более 100 тыс. сотрудников, которые подали более 30 тыс. предложений, 13 тыс. из которых были внедрены. Экономический эффект составил более 4 млрд. рублей.

Кибербезопасность:

— запущен базовый функционал Security Operations Center, реализующий систему коллективной защиты банковского сообщества от киберпреступлений в реальном времени в концепции Cyber-Security-as-a-Service;

— более 100 млн транзакций в сутки проверяется онлайн.

«Сбербанк» в сотрудничестве с Федеральной службой безопасности (ФСБ) разрабатывает общероссийскую систему защиты от киберпреступников. Ей смогут воспользоваться и другие банки. Система будет разработана к 2018 году. Сейчас у «Сбербанка» есть центры кибербезопаности в пяти городах, где работают около тысячи специалистов, которые ежедневно регистрируют около 1 млн. инцидентов. Системой смогут

воспользоваться и другие российские банки, которые обращаются к «Сбербанку» за помощью в случае кибератаки.

Разрабатываемая банком платформа будет платной для других кредитных организаций. Предполагается, что в основу системы лягут разработки дочерней компании «Сбербанка» «Бизон», которая специализируется на выявлений нарушений прав финансово-кредитных организаций и тестировании систем кибербезопасности банка. Новая платформа может стать конкурентом для «Лаборатории Касперского» — единственной российской компании, специализирующейся на кибербезопасности, которая известна во всём мире.

При этом, не все банки будут готовы предоставить «Сбербанку» свои данные, опасаясь утечки клиентов. В то же время они признают необходимость сотрудничества в борьбе с кибератаками, которые становятся всё опаснее. Будет лучше, если управление [системой] возьмёт на себя третья сторона, чтобы избежать конфликта интересов. Регулятор Центробанк — это наиболее подходящий посредник.

Из основных характеристик защиты ДБО особое внимание обращается на универсальность мер и средств защиты вне зависимости от методов атак, на возможность адаптации системы защиты в соответствии с изменениями технологий ДБО и бизнес-процессов кредитной организации, а также на способность предотвращать нарушения ИБ автоматически.

Безопасность эксплуатации банковских систем усложняется для клиентов их низкой ИБ-культурой. В ближайшем будущем для обеспечения безопасности необходимо сделать акцент на средствах защиты клиентской среды, к которым можно отнести механизмы интеллектуального реагирования на факты мошенничества и инструменты усиленной аутентификации пользователей, подтверждающие легитимность операций системы. Подобные процедуры и политики позволят значительно снизить

риски хищения денежных средств со счетов пользователей в тех системах, где корректно реализованы эти механизмы.

В сфере кредитно-финансовой деятельности специалисты делают акцент на низком контроле используемых бизнес-процессов и недостаточную эффективность взаимодействия банков между собой и с правоохранительными органами, а также уязвимости в базовом ПО систем ДБО. Низкая защищенность систем банковского обслуживания, находящихся в эксплуатации, явно свидетельствует о необходимости внедрения процессов обеспечения безопасности на всех стадиях жизненного цикла приложений. Анализ защищенности систем и контроль устранения выявленных погрешностей необходимо проводить и во время ее активного использования клиентами банка на регулярной основе. То есть нужно уделять внимание корректной реализации механизмов защиты.

С развитием российской регулятивной базы будет усугубляться ответственность кредитно-финансовых организаций за возможные финансовые потери их клиентов, связанные в том числе с атаками на системы ДБО, и усилятся требования к защите информации в кредитно-финансовых компаниях, в том числе в отношении систем ДБО. По мере развития финансовых технологий и их инкорпорирования в банковский бизнес будут возрастать и риски в сфере ИБ, и требования к профильным управлениям и департаментам, что вызвано комплексным подход в решении этой проблемы.

# СПИСОК ЛИТЕРАТУРЫ

1. О банках и банковской деятельности в Российской Федерации: [Текст] Федеральный закон РФ от 02 декабря 1990 г. № 395-1.

2. О залоге: [Текст] Федеральный закон РФ от 29 мая 1992 г. № 2872-I.

3. О кредитных историях:[Текст] Федеральный закон РФ от 30 декабря 2004 г. № 218-ФЗ.

4. О порядке расчета и доведения до заемщика – физического лица полной стоимости кредита: [Текст] Указание ЦБ РФ от 13 мая 2012 г. № 2012-У.

5. О порядке расчета и доведения до заемщика – физического лица полной стоимости кредита:[Текст] Указание ЦБ РФ от 13 мая 2012 г. № 2012-У.

6. Гражданский кодекс Российской Федерации. Часть 2: [Текст] Федеральный закон РФ от 26 января 1996 г. № 14-ФЗ (с изм. и доп. от 01 января 2012 г.).

7. Азнабаева, Г.Х. Информационная безопасность в банках при дистанционном обслуживании [Текст] // Г.Х. Азнабаева, Н.Г. Ираева. В сборнике: Наука сегодня: реальность и перспективы. материалы международной научно-практической конференции. Научный центр «Диспут». – 2016. – С. 70 – 72.

8. Айтуганова, А.Х. Современные принципы информационной безопасности интернет-банкинга [Текст] // А.Х. Айтуганова, Р.Р. Хусамов. Ученые записки ИСГЗ. – 2016.№ 1 (14). – С. 20 – 25.

9. Балезина, И.В. Потребительское поведение в современном обществе: кредиты [Текст] / И.В. Балезина. Master's Journal. – 2014. № 1. – С. 321-325.

10. Переверзева, Е.С. Банковская безопасность как одна из составляющих экономической безопасности государства [Текст] / Е.С. Переверзева, Ю.Н. Погребенко //Фундаментальные исследования. – 2015. – - № 11-4. – С.810-814.

11. Илинич, Е.В. Мошеннические операции с банковскими пластиковыми картами как угроза экономической безопасности в сфере банковской деятельности [Текст] / Е.В. Илинич // Статистика и Экономика. – 2013. – № 6. – С.41-45.

12. Фурманов, Д.В. Усугубление проблемы безопасности при использовании пластиковых карт [Текст] / Д.В. Фурманов, Е.Н. Смольянинова // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2012. – № 1. – С. 158-163.

13. Кривошапова, С.В. Оценка и способы борьбы с мошенничеством с банковскими картами в России [Текст] / С.В. Кривошапова, Е.А. Литвин // Международный журнал прикладных и фундаментальных исследований. – 2015. – № 4-1. – С. 116-120.

14. Барыбин, В.В. О механизме регулирования кредитных рисков в условиях нестабильности экономической конъюнктуры [Текст]// под ред. Барыбин В.В., Крыксин Г.В. Деньги и кредит. – 2011. – № 3. – С. 43 – 47.

15. Белоглазова, Г.Н. Банковское дело. Организация деятельности коммерческого банка [Текст]// Г.Н. Белоглазова, Л.П. Кроливецкая учебник. М.: Юрайт. – 2012 – 422 с.

16. Губенко, Е.С. О защите информации в национальной платежной системе [Текст] // Е.С. Губенко. Финансовое право. – 2016. – № 4. – С. 36 – 39.

17. Бердюгин, А.А. Обеспечение информационной безопасности дистанционного банковского обслуживания [Текст] // А.А. Бердюгин. В сборнике: Безопасные информационные технологии (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции. Под редакцией В.А. Матвеева. – 2016. – С. 58 – 61.

18. Гришина, Е.А. Тенденции развития кредитных услуг, предоставляемых коммерческими банками. [Текст]// Е.Г. Гришина. Финансы и кредит. – 2016. – № 28 (700). – С. 18 – 27.

19. Езангина И.А. ДБО: Современные угрозы финансового мошенничества [Текст] // И.А. Езангина, О.В. Шумилина. Сборник статей победителей VI Международной научно-практической конференции. Под общей редакцией Г.Ю. Гуляева. – 2017. – С. 12 – 15.

20. Земцова, Л.Н. Доступность банковских услуг как фактор информационной безопасности банковской деятельности [Текст] // Л.Н. Земцова. Информационная безопасность регионов. – 2015. – № 4 (21). – С. 92 – 95.

21. Иванов, И.Н. Социальные процессы формирования информационного общества и методы их измерения [Текст] // И.Н. Иванов. В сборнике: Технологии информационного общества X Международная отраслевая научно-техническая конференция: сборник трудов. – 2016. – С. 309 – 310.

22. Ильин, И.Е. В законе о потребительском кредите ставка сделана на баланс интересов [Текст]// И.Е. Ильин. Аудитор. – 2014. – № 2 (228). – С. 12 – 16.

23. Капустина, Н.С. Разработка стратегии потребительского кредитования в коммерческом банке как инструмент расширения спроса. [Текст]// Н.С. Капустина. Научно-методический электронный журнал Концепт. – 2017. – Т. 4. – С. 176 – 183.

24. Карпов, А.С. Совершенствование мер защиты информации при дистанционном банковском обслуживании [Текст] // А.С. Капов. Научные записки молодых исследователей. – 2017. – № 4. – С. 40 – 45.

25. Клочко, О.С. Различные схемы автоматизации и передачи дистанционных банковских операций [Текст] // О.С. Клочко, А.В. Чевычелов. Электронный журнал: наука, техника и образование. – 2017. – № СВ1 (11). – С. 121 – 124.

26. Кудрявцева, Ю.В. Инновационные финансовые технологии и операционные риски в сфере дистанционного банковского обслуживания [Текст] // Ю.В. Кудрявцева. Финансовая аналитика: проблемы и решения. – 2017. – Т. 10. – № 6 (336). – С. 647 – 662.

27. Кульбит, Е.В. Анализ системы электронного банкинга, как компонента системы дистанционного банковского обслуживания [Текст] // Е.В. Кульбит. Экономика. Бизнес. Банки. – 2017. Т. 2. – С. 104 – 110.

28. Макаров, В.Ю. Уточнение требований к оценке кредитоспособности заемщика Известия Саратовского университета. [Текст] // В.Ю. Макаров. Новая серия. Серия: Экономика. Управление. Право. – 2017. – Т. 17. – № 1. – С. 76 – 80.

29. Мухачева, Е.С. Совершенствование понятия договора присоединения в контексте новелл ФЗ «О потребительском кредите» [Текст] // Е.С. Мухачева. В сборнике: Правовые проблемы укрепления российской государственности Сборник статей. Редакторы: В.М. Лебедев, Г.Л. Осокина, С.К. Соломин, В. С. Аракчеев. – 2015. – С. 27 – 28.

30. Портал банковского анализа банков [Электронный ресурс]// http://analizbankov.ru/bank.php?BankId=vtb-24-1623&BankMenu=rating_pos.

31. Прохоров, И.Л. Единое информационное пространство для систем дистанционного банковского обслуживания [Текст] // Л.И. Прохоров. В сборнике: Приоритетные научные направления: от теории к практике

сборник материалов XXXIX Международной научно-практической конференции . 2017. С. 188 – 194.

32. Пузанов, В Е. Проблемы обеспечения информационной безопасности систем дистанционного банковского обслуживания кредитно-финансовых организаций с разветвленной сетью филиалов [Текст] // В.Е.Пузанов Современные материалы, техника и технологии. – 2016. – № 1(4). – С 178 – 184.

33. Русина, В.В. Банковское кредитование (потребительские кредиты) в условиях санкций [Текст] // В.В. Русина. В сборнике: Современные проблемы гуманитарных и естественных наук материалы XXI международной научно-практической конференции. Научно-информационный издательский центр "Институт стратегических исследований". – 2014. – С. 143 – 146.

34. Савельев, М.А. Проблемы информационной безопасности в системах дистанционного банковского обслуживания [Текст] // М.А. Савельев, В.В. Крепалов. Материалы ежегодной научно-практической конференции памяти Дага Хаммаршельда. – 2016. Т.2 – С. 185 – 189.

35. Сажнева, С.В. Потребительские кредиты российских банков: анализ рейтинга и условий предоставления кредитов [Текст] // Сажнева С.В., Таранушич Д.М. В сборнике: Стратегическое и проектное управление сборник научных статей. ООО «Парма-Телеком». Пермь. – 2014. – С. 177 – 180.

36. Самочетова, Н.В. Дистанционное банковское обслуживание в России на пути его развития [Текст] // Н.В. Самочетова, Н.Н. Мартыненко. Современная наука: актуальные проблемы теории и практики. Серия: Познание. – 2016. – № 5-6. – С. 49 – 54.

37. Середа, А.В. Новеллы в гражданско-правовом регулировании потребительского кредитования в свете принятия федерального закона «О

потребительском кредите» [Текст]// А.В. Середа. Новый юридический журнал. – 2014. – № 3. – С. 75 – 80.

38. Согов,. М.Р. Меры информационной безопасности дистанционного банковского обслуживания [Текст] // М.Р. Согов. В сборнике: Инновационные технологии научного развития. Сборник статей международной конференции: в 5 частях. – 2017. – С. 89 – 91.

39. Соколова, Т.Н. Оценка информационной безопасности систем дистанционного обслуживания [Текст] // Т.Н. Соколова, В.С. Васильев. Информационная безопасность регионов. – 2017. – № 2 (27). – С. 34 – 39.

40. Синцов, Г.В. Пробелы в законодательстве о потребительском кредите [Текст]// Г.В. Синцов. Российская юстиция. – 2015. – № 9. – С. 18 – 20.

41. Сиротский, А.А. Анализ типовых угроз информационной безопасности автоматизированных систем применительно к дистанционному банковскому обслуживанию [Текст] // А.А. Сиротский В сборнике: Информационная безопасность бизнеса и общества. Сборник изобретательных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский государственный социальный университет. Москва. – 2016. – С. 40 – 45.

42. Скляров, И.Ю., Склярова, Ю.М., Лапина, Е.Н. Совершенствование методических подходов к оценке и управлению банковскими рисками. [Текст]// И.Ю. Скляров, Ю.М. Склярова, Е.Н. Лапина. Экономика и предпринимательство. – 2016. – № 2-1 (67-1). – С. 540 – 546.

43. Столбовская, Н.Н. Особенности работы банков с проблемными потребительскими кредитами [Текст] // Н.Н. Столбовская, Т.Р. Омельянченко. Вестник научных конференций. – 2016. –№ 1-5 (5). – С. 182 – 184.

44. Тарасова, Н.В. Потребительский кредит: новое в правовом регулировании [Текст] // Н.В. Тарасова, И.Г. Бабаева И.Г. В

сборнике: Актуальные вопросы юридических наук Материалы II Международной научной конференции. – 2015. – С. 79 – 82.

45. Топалов, Р.В. Угрозы безопасности систем дистанционного банковского обслуживания [Текст] // Р.В. Топалов, Т.Г. Чачуа. Научные записки молодых исследователей. – 2017. – № 2. – С. 63 – 66.

46. Фурзикова, Е.Г. Оценка эффективности работы методов управления проблемными потребительскими кредитами в коммерческом банке [Текст] // Е.Г. Фурзикова. Фундаментальные исследования. – 2013. – № 1-2. – С. 514 – 519.

47. Хоменко, Е.Г. Работа банков с просроченными потребительскими кредитами [Текст] // Е.Г. Хоменко. Право и экономика. – 2014.– № 7 (317). – С. 32 – 36.

48. Центральный Банк России. [Электронный ресурс]// URL: www.cbr.ru.

49. Чернавин, Ф.П. Применение комитетных конструкций для принятия решений по потребительским кредитам [Текст] // Ф.П. Чернавин. Экономика и предпринимательство. – 2015. – № 12-4 (65-4). – С. 143 – 149.

50. Чернавин, Ф.П. Применение нейронных сетей к задачам оценки вероятности дефолта по потребительским кредитам [Текст] // Ф.П. Чернавин. Журнал научных публикаций аспирантов и докторантов. – 2013. – № 7 (85). – С. 21 – 25.

51. Юсупова, О.В. Безопасность транзакций при использовании интернет-банкинга [Текст] // О.В. Юсупова. Финансовая аналитика: проблемы и решения. – 2016. – № 35 (317). – С. 26 – 40.

52. Кешелаева А.В. Введение в цифровую экономику. [Текст] А.В., Кешелаева. 2017.– С.24-26.

53. Путин В.В. Арифметика будущего. [электронный ресурс] режим доступа ://rg.ru/2017/07/05/putin-sravnil-cifrovuiu-ekonomiku-s-elektrifikaciej.html.

54. Путин В.В. Без цифровой экономики нет будущего. [электронный ресурс] режим доступа :http://www.vestifinance.ru/articles.

55. Утверждение цифровой экономики. [электронный ресурс] режим доступа: http://www.vestifinance.ru/articles.

56. Цифровая экономика 2017. [электронный ресурс] режим доступа: http://www.vestifinance.ru/articles.

57. Дяченко О.А. Возьми мой риск! [Электронный ресурс]// Национальный банковский журнал. Режим доступа: URL: http://www.klerk.ru/bank/articles/209576.

58. Евстигнеева, А. 0% переплаты: как не запутаться в условиях по кредиту [Электронный ресурс]// URL: http://lf.rbc.ru/potreb/2017/02/14.

59. Евстигнеева, А. Банки открывают сезон дорогих кредитов [Электронный ресурс]// URL http://lf.rbc.ru/potreb/2017/02/13.

60. Сбербанк России. [Электронный ресурс]// режим доступа - URL: www.sberbank.ru.

61. Шире сеть! [Электронный ресурс]// URL: http://www.alfabank.ru/ press/monitoring /2017/5/ 11/1.

62. Янов ,В.В. Современные тенденции кредитования физических лиц в РФ [Электронный ресурс]// Теория и практика общественного развития. 2012. № 12. URL: http://www.teoria-practica.ru/pdf.

63. Безопасность. // bankdbo.ru – [Электронный ресурс] – Режим доступа. – URL: http://www.bankdbo.ru/bezopasnost.

64. Информационная безопасность ДБО. // PCWeek – [Электронный ресурс] – Режим доступа. – URL: https://www.itweek.ru/security/article/detail.php?ID=148306.

65. Обзор основных уязвимостей онлайн-банков. // ИТ-сектор– [Электронный ресурс] – Режим доступа. – URL: https://itsektor.ru/obzor-osnovnyx-uyazvimosteyi-onlayin-bankov.html.

66. Пискунов И. Особенности обеспечения информационной безопасности в банковской системе. – [Электронный ресурс] – Режим доступа. – URL: https://www.antimalware.ru/analytics/Technology_Analysis/Features_information_security_in_the_banking_system.

67. Системы дистанционного банковского обслуживания (рынок ДБО России). // Tadvicer.ru – [Электронный ресурс] – Режим доступа. – URL: http://www.tadviser.ru/index.php.

68. Уязвимости онлайн-банков 2016: лидируют проблемы авторизации. // habrahabr.ru – [Электронный ресурс] – Режим доступа. – URL: https://habrahabr.ru/company/pt/blog/307450/.

# ПРИЛОЖЕНИЯ