**Преподаватель**

**гбпоу ао «агкпт»**

**Трдатян Алина**

**СОВРЕМЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ БАНКОВ**

**АННОТАЦИЯ**

На современном этапе систематизированы новые программные средства и технологии, используемые в дистанционном банкинге. Тем не менее уязвимостей, различных отклонений и программных сбоев меньше не становится.

Кроме того, постоянный контакт с банком отнимает много времени, отвлекает сотрудников банка от обработки больших объемов данных и увеличивает вероятность сбоев в работе операционных систем банка. В этом контексте экономические отношения, возникающие в процессе онлайн-обслуживания, и способы обеспечения их защиты являются предметом настоящего исследования.

**Ключевые слова:** информационная безопасность, банковская сфера, банк, клиент, счет, услуга, SQL, безопасность данных, информационная безопасность банков, Российская Федерация.

**Keywords**: information security, banking, bank, client, account, service, SQL, data security, information security of banks, Russian Federation.

На современном этапе развитый в технологическом плане банк отличает широкая номенклатура услуг банковского маркетинга. Среди этой номенклатуры особо следует выделить кредитование юридических и физических лиц, используемые в отношении которых кредитные продукты составляют ключевое направление работы банков. Другие формы работы имеют меньшую востребованность сделки по трастам, инвестициям, а также международные расчеты.  Не прекращается работа, связанная с поиском инновационных форм работы с потенциальными клиентами. Работа с дебетовыми и кредитными картами в сочетании с дистанционными способами обслуживания клиента расширяют возможности для коммуникации с клиентами, банками, поддерживаемыми операторами мобильной связи. Подобные инновации в значительной степени способствуют экономической эффективности банковских операций. Особенное значение для маркетинга банков имеет расширение ассортимента дистанционных банковских услуг, выгодный для всех участников взаимодействия. Главное этому объяснение – снижения лишней цепочки контактов, экономия затрат времени на организацию расчетов.

Комплексная система защиты информации (КСЗИ) – это совокупность организационных и инженерно-технических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки, несанкционированного доступа и модификации[[1]](https://www.evkova.org/kursovye-raboty/sistema-zaschityi-informatsii-v-bankovskih-sistemah-------#footnote-1). Создание КСЗИ, в соответствии с требованиями системы нормативных документов России в области технической защиты информации, обусловлено необходимостью обработки предприятием информации с ограниченным доступом на компьютерах, не подключенных к сети, и в сетях предприятия.

В наиболее общем виде подобные стратегии учитывают реализацию системы мероприятий в банковском учреждении:

* создание информационных центров обработки данных для предотвращения угроз информационной безопасности;
* повышение мощности серверов для обработки банковской информации;
* обеспечение омниканального взаимодействия с клиентами для охвата всех клиентских операций с банком, а также решение задач бизнеса в отдаленных географических регионах.

Структура систем обработки информации в системах банковского дистанционного обслуживания представлена такими компонентами, как: 1) рабочее место оператора; 2) устройства, позволяющие интегрировать воедино цифровые показания и аудио сигналы; 3) устройства, позволяющие регистрировать голоса, запоминать их, и обеспечивать контроль доступа к системе.

Дистанционный доступ к управлению личной учетной записью обеспечивается посредством мобильных цифровых устройств, интернет-коммуникаций. Следует полагать, в рамках данной публикации нет особой необходимости их перечислять, так как они детально изучены и представлены не в одной сотне научных публикаций.

В значительной степени расширяет возможности банков адаптация дистанционных банковских продуктов к конфигурации интернет-браузеров, применяемых, как на мобильных устройствах, так и на стационарных компьютерах и ноутбуках. Такая организованная коммуникация обеспечивается защищенным соединением Secure Sockets Layer, позволяющим эффективно организовать обмен данными между банком и клиентом.

Кроме официально установленных правил и процедур, банк обеспечивает клиентов требуемыми сведениями, определяющими принципы сотрудничества с банком конкретной организационно-правовой формы (АО и ПАО). В частности, речь идет о выборе клиентом системы безопасности, необходимой для предотвращения несанкционированного доступа к электронным счетам клиентов.

Базовым условием организации системы защиты банковской информации является использование процедур идентификации и аутентификации. Обеспечение реализации данных процедур банковского контроля является отличает большое количество известных способов, которые непрерывно развиваются и совершенствуются. В частности, применение карт с непостоянным одноразовым паролем либо многоразовым паролем представляется в качестве возможного эффективного способа аутентификации. Возможным вариантом аутентификации является протекция посредством криптографического ключа для мобильных устройств, куда при таком подходе отправляется смс с паролем для доступа к информационной системе. Другим вариантом является организация защиты посредством так называемых токенов – цифровой сертификат по обязательствам компании. В данном случае доступ к личным данным обеспечивается посредством распознавания клиентов по отпечаткам пальцев.

Большинство банков, перешедших на дистанционное обслуживание клиентов, используют в своей работе Digital Light Processing, обеспечивающий доступ клиентов к базам данных пользователей, имеющих легальный доступ к банковским коммуникациям. Также для задач банковской безопасности применяются такие антивирусные продукты McAfee, Juniper, Balabit, Good for Enterprise многие другие известные.

Так, например, использование такой программы, как Imperva Database Security, позволяет обеспечивать контроль доступа к клиентским базам данных. Взаимодействие данной программы с клиентским системами позволяет сравнивать нормативы клиентского поведения с наблюдаемыми отклонениями. Кроме того, возможности программы обеспечивают контроль запросов администраторов и пользователей в пределах базы данных: прежде всего, речь идет о контроле использования данных, об использовании прав доступа и об оценке уязвимостей.  Ведущими критериями оценки эффективности данной технологии выступают такие характеристики, как гибкость использования, минимальные трансформации инфраструктуры в ходе внедрений этой технологии, низкие издержки на обустройство, внедрение, эксплуатацию, а также несложное администрирование.

Интеграция возможностей двух принципиально разных Mobile Device Management и Bring Your Own Device позволяет обеспечить новые качества информационной безопасности для мобильных банков, делая взаимодействие пользователей смартфонов и банков более безопасным.

Bring Your Own Device по своей сути представляет вариант организации рабочего места сотрудника посредством применения персонального устройства для доступа к ресурсам и коммуникациям банка. Общая группа технологий BYOD обеспечивает категоризацию пользователей и персонала для учета их на этапе аутентификации, а также на их основе проектировать и организовать иерархическую политику доступа к корпоративным ресурсам, что позволяет идентифицировать тип устройства для входа пользователя в сеть, а также проводимые в ней операции.

Применение Mobile Device Management обеспечивает банковскому персоналу большую мобильность и эффективность организации работы вне физических границ офиса для использования служебной электронной почты. Структура данной технологии состоит из 2 элементов: центр управления и клиентского программного обеспечения, необходимого для шифрования конфиденциальной информации, а также хранения пришедших на рабочую почту писем и сообщений. Такой охраняемый почтовый ящик представлен такими элементами, как почтовый ящик, даты и события. Банковский сервер обеспечивает передачу почты в основной модуль посредством защищенного узла [11, с. 6].

В целях обеспечения безопасности технологии Mobile Device Management предусматривают ситуации, когда персональные мобильные устройства сотрудников могут быть похищены, либо утеряны. Для этого администраторы могут оперативно реагировать посредством данной технологии. В подобных ситуациях администраторы оперативно уничтожают все файлы на носителях и устройствах, а, если потребуется, персональные устройства будут заблокированы, а данные удалены. Следует подчеркнуть, систему подобных действий реализуется посредством специальных команд, отправляемых на персональные устройства. К тому усложняют доступ к почтовыми ящику и связанных с ним элементам разноуровневые сложные пароли. К тому же технологии данной группы интегрируют в себе антивирусные программы, что позволяет им выступать составной частью более масштабных комплексных систем защиты информации, среди которых наиболее известными и эффективными признаны экспертами следующие продукты Mobile Device Management: Good for Enterprise, McAfee, SAP, MobileIron [11, с. 6].

Однако, как подчеркивают эксперты, даже занимающие высокие рейтинговые места программные продукты не лишены недостатков. Слабое звено Mobile Device Management связано с оперативной обработкой данных. В процессе увеличения масштабов работы лица, уполномоченные заниматься информационной безопасностью сталкиваются со значительными проблемами анализа угроз, а также их профилактики.

Решить проблемы и выйти на новый уровень в администрировании информационной безопасности позволяют технологии группы Security Information and Event Management, ориентированные на профилактику отклонений в информационной безопасности посредством системы специальных критериев. Ключевыми задачами технологии Security Information and Event Management выступают следующие: 1) консолидировать и сохранить журналы событий из дифференцированных источников; 2) распределить и обработать события согласно правилам; 2) оповестить и предоставить в автоматическом режиме инструменты с целью анализа и экспертизы инцидентов.

Ключевой технологией, необходимой для анализа угроз информационной безопасности предприятия, выступает HP ArcSight ESM. Возможности данной технологии позволяют администраторам контролировать адреса e-mail, учетные записи по каждому пользователю, и формировать отчетность по всем их действиям в информационной системе.  Необходимо признать, возможности данной технологии вполне можно эксплуатировать в банковских учреждениях.

Тенденции ускорения технологических циклов систем безопасности не обходят стороной и банковский сектор, и финансово-кредитные учреждения – основной потребитель данных технологий. Равновесие в безопасности данных становится в новых условиях ключевой задачей администратора. Именно внедрение инноваций для управления рисками является серьезным конкурентным преимуществом финансово-кредитных учреждений, определяющим доверие целевой аудитории.

Существующие подходы к информационной безопасности для виртуального банкинга быстро морально устаревают при высокой конкуренции инноваций. Одной из подобных инноваций выступает «домашний банкинг». Применение этой цифровой технологии повышает риски нелегального доступа и нарушения функционирования инфраструктуры, и повышает требования к системам обработки и защиты информации (идентификация, аутентификация, токен, криптографический ключ). Одним из подобных требований является адаптация банковского продукта к конфигурации интернет-браузера на мобильных устройствах.

Анализ современных тенденций дистанционного банковского обслуживания и развития виртуального банкинга в российских банках показывает, что активное применение находят следующие технологии (самостоятельные технологии – Digital Light Processing, Imperva Database Security), (взаимодополняющие – Mobile Device Management, Bring Your Own Device, Security Information and Event Management HP ArcSight ESM). Несмотря на слабые места каждой и технологий, они применимы в банковском секторе.

**Список литературы:**

1. Банковские информационные системы и технологии. Часть 1. Технология банковского учета. - М.: Финансы и статистика, 2015. - 384 c.
2. Беленькая, М. Н. Администрирование в информационных системах / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. - М.: Горячая линия - Телеком, 2011. - 400 c.
3. Бионические информационные системы и их практические применения / Коллектив авторов. - Москва: ИЛ, 2011. - 796 c.
4. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2013. - 368 c.
5. Вдовенко, Л. А. Информационная система предприятия / Л.А. Вдовенко. - М.: Вузовский учебник, Инфра-М, 2012. - 240 c.
6. Грекул, В.И. Автоматизация деятельности предприятия розничной торговли с использованием информационной системы Microsoft Dynamics NAV / В.И. Грекул. - М.: Бином. Лаборатория знаний, 2014. - 100 c.
7. Ивлев, В. А. ABIS. Информационные системы на основе действий / В.А. Ивлев, Т.В. Попова. - М.: 1С-Паблишинг, 2012. - 248 c.
8. Избачков, Ю. Информационные системы / Ю. Избачков, В. Петров. - Москва: СИНТЕГ, 2016. - 656 c.
9. Информационная система математических Интернет-ресурсов MathTree / Коллектив авторов. - Москва: Мир, 2017. - 353 c.
10. Информационные системы - миф и действительность. - М.: Знание, 2014. - 433 c.