Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Защита информации в сервисе онлайн банкинга на примере ПАО "Сбербанк"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 431
_____ Панкратов, И. Е.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Общество 21 века можно назвать информационным, ведь сегодня информация играет очень большую роль в жизни каждого из нас. Интернет продолжает захватывать уголки нашего мира каждую секунду, а вместе с ним наблюдается постоянный прирост информации. Исходя из этого можно смело заявить, что возрастает необходимость защищать её.

Для того, чтобы злоумышленники не смогли получить несанкционированный доступ, следует разрабатывать комплексную систему защиты информации. Её главной задачей является обеспечение информационной безопасности, построенной на специальных программных решениях, мероприятиях и методах.

Каждая организация имеет свои секреты, которые знает только она. Утечка любого рода информации может катастрофически сказаться на самой организации. Она может понести колоссальные финансовые потери, в следствии, например, получения конфиденциальных данных третьими лицами.

Так, хищение логина и пароля сотрудника банка от какой-либо программы, которая работает с защищенными данными, может повлечь не только потерю конфиденциальной информации организации, но и потерю информации физических и юридических лиц, обсуживающихся у банка. Для того, чтобы избежать данных инцидентов, необходимо проводить мероприятия по защите информации. Однако очень часто предприятия забывают про контроль целостности данных, поддержания определенных уровней защиты и их совершенствования.

Исходя из законодательства РФ, организация обязана проводить модернизацию система защиты. Для этого необходимо проводить специальные мероприятия по анализу, выявлять новые угрозы и уязвимости , которые появляются каждый день, анализировать информационные системы на утечки. После проведения детального анализа, необходимо составить техническое задания для модернизации комплексной системы защиты информации, где должны будут отображены такие

детали как: требования, список мероприятий, оценка рисков и затрат, оценка эффективности.

В данной работе я хочу проанализировать систему онлайн-банкинга ПАО «Сбербанк» на предмет угроз, уязвимостей и защищенности.

ГЛАВА 1 . АНАЛИЗ СЕРВИСА ОНЛАЙН-БАНКИНГА НА ПРИМЕРЕ ПАО «СБЕРБАНК»

1.1. История банка

1841 - 1895 годы: основание и развитие банковского дела в России.

12 ноября 1841 года российским императором Николаем I был подписан указ об учреждении в России сберегательных касс «для доставления через то средств к сбережению верным и выгодным способом». Эта дата стала считаться днем рождения ПАО «Сбербанк».

Самым первым клиентом первого банка страны стал надворный советник Николай Антонович Кристофари, на свой счет он внес внушительную по тем временам сумму в 10 рублей и стал обладателем сберегательной книжки.

Правительственные органы России проводили активную агитационную работу для того, чтобы объяснить населению страны основные преимущества хранения средств в сберегательном банке. Первая российская реклама оказалась эффективной: если в 1842 году сберегательная касса обслуживала в среднем 70 вкладчиков в день, то к 1860 году более 500 человек.

ПАО «Сбербанк» изначально взял курс на масштабную работу со всеми слоями населения страны: среди его вкладчиков были крестьяне, дворянство, купцы, военные, чиновники и даже духовенство.

1895 - 1917 годы: «золотой век» первого банка России и развитие финансовой грамотности населения.

Расцвет банковского дела в России пришелся на 1865 - 1895 гг. За этот период количество сберегательных касс на всей территории страны увеличилось с 47 до 3875, а число выданных сберегательных книжек превысило 2 миллиона.

1 июня 1895 года стало поворотной датой в истории российского банковского сектора. Именно в этот день был принят новый Устав сберегательных касс, кото-

рый гарантировал каждому сохранение его коммерческой тайны. Кроме того появилось и разнообразие в типах вкладов: можно было открыть сберегательный счет на ребенка или на погребение.

1917 -1941 годы: глобальные перемены в политике ПАО «Сбербанк».

Начало XX века ознаменовалось для России бурными и масштабными потрясениями: Первая мировая война, революция, Гражданская война. Однако ни одно из этих событий не смогло замедлить активного развития ПАО «Сбербанк».

В кризисные для страны времена ПАО «Сбербанк» смог сохранить вложения своих вкладчиков, объявив их неприкосновенными. Но не обошлось и без негативных последствий - коммерческая тайна, фактически, была упразднена: правительство издало указ, обязывающий сберегательные кассы предоставлять государственным органам информацию о состоянии счета любого вкладчика.

Новая экономическая политика России повлекла за собой и серьезные изменения в банковской структуре: сберкассы стали осуществлять денежные переводы, выпускать собственные заемные сертификаты, проводили операции с процентными и ценными бумагами.

1941 - 1953 годы: ПАО «Сбербанк» в годы Великой Отечественной войны и послевоенное время, участие в проектах государственного значения.

ПАО «Сбербанк» продолжал развиваться и содействовать обществу и в это время. Для привлечения средств он организовывал лотереи для населения и занимался размещением государственных займов.

Важнейшим видом деятельности ПАО «Сбербанк» в 1941 - 1945 и последующие годы является сотрудничество с государством в сфере атомной и ядерной промышленности. Помощь ПАО «Сбербанк» в привлечении средств и финансирование разработок позволило стать России лидером в сфере производства и переработки ядерного топлива и оставаться им и по сей день.

Учрежден новый Устав государственных сберкасс.

1953 - 1991 годы: развитие и преобразование ПАО «Сбербанк» во времена «оттепели», «застоя» и «перестройки».

Несмотря на сложность первых послевоенных лет, начиная уже с 50-ых годов, ПАО «Сбербанк» продолжил свое стремительное и устойчивое развитие. За 30 лет количество сберегательных касс увеличилось вдвое (с 40 тысяч до 79 тысяч), количество клиентов банка возросло в 12 раз, а сумма их вкладов показала рекордные темы роста, увеличившись в 100 раз.

ПАО «Сбербанк» активно участвовал в восстановлении разрушенной войной инфраструктуры страны – были заново построены и отремонтированы дороги и трассы федерального значения. Сегодня ПАО «Сбербанк», сохраняя традиции, продолжает развивать программы дорожного строительства в России.

В 1987 году в рамках перестроечных реформ сберегательные кассы были реорганизованы в Сберегательный Банк СССР – так знакомый нам финансовый институт получил известное на весь мир название. Уже в 1989 году начал работать первый банкомат ПАО «Сбербанк» и в том же году банк стал членом Всемирного института сберегательных банков.

1991 год ознаменовался распадом СССР, но ПАО «Сбербанк» сохранил свои функции и остался единственным банком на всем бывшем постсоюзном пространстве, который продолжал работать.

1991 - 2008 годы: глобальные перемены ПАО «Сбербанк» - жизнь по новым экономическим законам.

В период с 1991 года по 2008 год ПАО «Сбербанк» претерпел существенные изменения, пережил кризис и окончательно сформировался как современный и универсальный банк, открытый для работы со всеми группами клиентов, опора и поддержка Российской экономики.

В 1991 году общим собранием акционеров был учрежден Акционерный Коммерческий Сберегательный Банк Российской Федерации, а в 1993 году в Московских отделениях начали функционировать первые банкоматы.

В 1995 году был создан Негосударственный пенсионный фонд ПАО «Сбербанк». Благодаря профессиональному инвестированию пенсионных средств, накопленная за 10 лет доходность НПФ составила 278%.

В 2001 году началось сотрудничество ПАО «Сбербанк» и Олимпийского комитета. Главный банк страны поддерживал российских спортсменов на играх в Солт-Лейк-Сити (2002), Афинах (2004) и Турине (2006).

В 2002 году ПАО «Сбербанк» выпустил первые карты VISA «Аэрофлот» — задача этого проекта состояла в том, чтобы сделать внутренние и международные полеты россиян комфортными и экономически привлекательными. Высокий спрос на карты ПАО «Сбербанк» «Аэрофлот», который сохраняется и сегодня, подтверждают эффективность этого проекта.

В 2003 году началось плодотворное сотрудничество ПАО «Сбербанк» и Северного флота России. Благодаря ему сегодня военнослужащие, их семьи и гражданский персонал получили доступ к широкому спектру банковских услуг и получили возможность кредитования на льготных условиях.

В 2006 ПАО «Сбербанк» реализует свою политику расширения на международных рынках и открывает представительство в Казахстане, а 28 ноября 2007 Греф Г.О. утвержден Председателем Правления ПАО «Сбербанк». 21 октября 2008 года Наблюдательный Совет ПАО «Сбербанк» единогласно одобрил стратегию «Развитие Сбербанка до 2014 года».

Разработана Производственная Система ПАО «Сбербанк» (ПСС), основанная на технологии продуманного и экономичного производства.

В 2008 начала работать услуга Сбербанк Онлайн, благодаря которой клиенты банка в Московском регионе могут круглосуточно в Интернете совершать банковские операции.

Внедрен новый проект «Кредитная фабрика», ключевой особенностью которого является автоматизация процесса принятия решения о выдаче кредита.

В декабре 2008 года ПАО «Сбербанк» выпустил благотворительную карту «Подари жизнь» с которой прибыль ПАО «Сбербанк», полученная от клиентов

банка за обслуживание карты, а так же проценты за совершенные им покупки, отчисляется в помощь детям, страдающим тяжелыми онкологическими и гематологическими заболеваниями.

2009 год: деятельность и меры ПАО «Сбербанк» в тяжелой финансовой ситуации: кризис преодолен.

2009 год стал отправной точкой в масштабном развертывании и реализации «Стратегии развития Сбербанка до 2014 года». Параллельной, но немаловажной задачей для банка стало оказание помощи обществу в решении проблем, вызванных мировым финансовым кризисом, и стабилизации их финансового положения.

Обновлены и расширены услуги, которые банк предлагает частным лицам. Пересмотрены и улучшены программы кредитования, снижены процентные ставки. Разработан Универсальный договор обслуживания, благодаря которому каждый клиент смог получить доступ ко всем услугам банка. Было создано специальное подразделение для работы с гражданами, чей ежемесячный доход не превышает 25 тысяч рублей.

Начала свою работу система «Кредитное страхование».

ПАО «Сбербанк» приступил к реализации проекта «Обслуживание состоятельных клиентов». В октябре ПАО «Сбербанк» начал обслуживать карты MasterCardPlatinum, VISA Platinum и VISA Infinite.

Банк предоставил клиентам новый вид брокерских услуг на фондовом рынке интернет - торговли с использованием системы удаленного доступа Focus IV Online.

Проведены масштабные работы по поддержке предпринимательской деятельности и созданы новые услуги для корпоративных клиентов.

Идет активная стимуляция и поддержка малого бизнеса. Разработаны новые кредитные программы: «Бизнес-авто», «Коммерческая недвижимость», «Экспресс-лизинг» и «Микрокредит субъектам малого бизнеса».

В подразделениях банка в Москве и Самаре начала работать система Сбербанк бизнес Онлайн.

Активно развивается инфраструктура ПАО «Сбербанк», а в конце 2009 ПАО «Сбербанк» успешно завершает ребрендинг.

В Москве открывается уникальный, инновационный и высокотехнологичный «Офис будущего Сбербанка», идет подготовке к открытию 20 аналогичных офисах в 8 городах России.

Внедрены проекты по оптимизации операционной деятельности банка.

Создан Корпоративный университет ПАО «Сбербанк», базовыми принципами которого стало сотрудничество с ведущими международными бизнес-школами.

Подготовлен проект создания Высшей международной банковской школы.

Идет активное формирование кадрового резерва банка: поиск молодых талантливых специалистов и развитие их потенциала.

Создана единая служба мониторинга и контроля работоспособности банкоматов в Москве, оптимизирован процесс доставки денежной наличности клиентам и офисам банка в Москве.

Завершился процесс реорганизации информационно-технологических служб банка.

Внедрена автоматическая система управления взаимоотношениями с клиентами - юридическими лицами.

Разрабатывается проект создания платформы для комплексного анализа деятельности банка.

Запущена новая модель обслуживания клиентов - программа «Базовый продукт», позволяющая сместить фокус с продажи отдельных продуктов на комплексное обслуживание клиента.

Развернута система управления единым профилем клиента по физическим лицам Москвы — «MDM-система».

Укрепляются позиции ПАО «Сбербанк» на российском и международном рынках.

ПАО «Сбербанк» вошел в топ-20 крупнейших банков по рыночной капитализации.

Получено разрешение на открытие филиала ПАО «Сбербанк» в Индии, Нью-Дели.

ПАО «Сбербанк» стал победителем в ряде номинаций ежегодного мероприятия «Российские лидеры в сфере корпоративного управления».

Идет активное развитие благотворительной деятельности банка, выпущена «Социальная карта» ПАО «Сбербанк».

ПАО «Сбербанк» стал генеральным партнером Олимпийских игр «Сочи-2014».

2010 год: новый этап в истории ПАО «Сбербанк»: внедрение инновационных решений, новые программы и прогрессивные технологии

В 2010 году продолжилось устойчивое развитие ПАО «Сбербанк», был заключен ряд стратегически важных договоров, проведена аттестация и оценка работающего персонала, приняты дополнительные меры по улучшению качества обслуживания граждан, реализованы социально-значимые и экономические проекты.

ПАО «Сбербанк» отменил все комиссии за рассмотрение и выдачу кредитов, дважды были снижены процентные ставки кредитования.

Создана Служба Заботы о клиентах ПАО «Сбербанк», призванная оперативно реагировать на жалобы, пожелания и комментарии клиентов.

Заключен договор между ПАО «Сбербанк» и профсоюзом, где зафиксированы принципы социальной ответственности банка за своих сотрудников.

1.2. ПАО «Сбербанк» в наши дни

В сегодняшнем ПАО «Сбербанк» почти ничего не напоминает о сберегательных кассах, функции которых он выполнял на протяжении значительного периода своей истории. Но удивительно другое: ПАО «Сбербанк» уже мало похож даже на самого себя всего лишь десятилетней давности.

Способность к переменам и движению вперед – признак отличной «спортивной» формы, в которой находится сегодня ПАО «Сбербанк». Титул старейшего и крупнейшего банка России не мешает ему открыто и добросовестно конкурировать на международном банковском рынке и «держать руку на пульсе» финансовых и технологических перемен. ПАО «Сбербанк» не только шагает в ногу с современными тенденциями рынка, но и опережает их, уверенно ориентируясь в стремительно меняющихся технологиях и предпочтениях клиентов.

Сегодня ПАО «Сбербанк» - это российский коммерческий банк, международная финансовая группа, один из крупнейших банков России и Европы. Контролируется Центральным Банком Российской Федерации. Полное наименование - Публичное акционерное общество «Сбербанк России».

ПАО «Сбербанк» - это кровеносная система российской экономики, треть ее банковской системы, дает работу и источник дохода каждой 150-й российской семье.

На долю лидера российского банковского сектора по общему объему активов приходится 29,4% совокупных банковских активов.

Банк является основным кредитором российской экономики и занимает крупнейшую долю на рынке вкладов. На его долю приходится 46,4% вкладов населения, 34,7% кредитов физическим лицам и 33,9% кредитов юридическим лицам.

ПАО «Сбербанк» сегодня – это 16 территориальных банков по всей стране, в 83 субъектах Российской Федерации, расположенных на территории 11 часовых поясов. По состоянию на 1 мая 2017 года число отделений ПАО «Сбербанк» составило 14 826.

Только в России у ПАО «Сбербанк» более 110 миллионов клиентов – больше половины населения страны, а за рубежом услугами ПАО «Сбербанк» пользуются около 11 миллионов человек.

Среди клиентов ПАО «Сбербанк» – более 1 млн предприятий (из 4,5 млн зарегистрированных юридических лиц в России). Банк обслуживает все группы корпоративных клиентов, причем на долю малых и средних компаний приходится более 35% корпоративного кредитного портфеля банка. Оставшаяся часть — это кредитование крупных и крупнейших корпоративных клиентов.

Спектр услуг ПАО «Сбербанк» для розничных клиентов максимально широк: от традиционных депозитов и различных видов кредитования до банковских карт, денежных переводов, банковского страхования и брокерских услуг.

Стремясь сделать обслуживание более удобным, современным и технологичным, ПАО «Сбербанк» с каждым годом все более совершенствует возможности дистанционного управления счетами клиентов.

В банке создана система удаленных каналов обслуживания, в которую входят:

1. Онлайн-банкинг Сбербанк Онлайн (более 30 млн активных пользователей).

2. Мобильные приложения Сбербанк Онлайн для смартфонов (более 18 млн активных пользователей).

3. SMS-сервис Мобильный банк (более 30 млн активных пользователей).

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

ПАО «Сбербанк» является крупнейшим эмитентом дебетовых и кредитных карт. Совместный банк, созданный Сбербанком и BNP Paribas, занимается POS-кредитованием под брендом Cetelem, используя концепцию «ответственного кредитования».

Сегодня Сбербанк является единственным из российских банков, который входит в Топ-50 крупнейших банков мира.

1.3. Автоматизированные банковские системы ПАО «Сбербанка»

ПАО «Сбербанк» делит свои АБС по 11 основным направлениям:

1. Автоматизированные системы ядра (Core banking).
2. Системы FrontEnd.
3. Процессинговые системы.
4. Системы типа CRM.
5. BI.
6. Кредитные системы.
7. Системы по управлению рисками.
8. Системы по управлению инвестициями.
9. Системы по управлению внутрихозяйственной деятельностью и персоналом.
10. Системы платформы BPM.
11. Системы ДБО.

Подробная информация о каждой АБС прикреплено в ПРИЛОЖЕНИИ А, а краткое описание по каждому из направлений изложено далее.

Автоматизированные системы ядра (Core banking):

Данные системы предназначены для обслуживания розничного сектора клиентов ПАО «Сбербанк» и ориентированы, в первую очередь, на обслуживание физических лиц. В числе операций, которые выполняются с их помощью – обеспечение хранения счетов по вкладам физических лиц и данных о клиентах, обслуживание запросов структурных подразделений отделений о состоянии счетов по вкладам физических лиц, прием банковских транзакций от функциональных подсистем операционного уровня и другие.

Системы FrontEnd:

Одной из центральных систем данного блока является АС ФС, позволяющая выполнять функции администрирования офисом, приема платежей и переводов, погашения кредита физических лиц, работы со счетами и вкладами, банковскими картами, сберегательными сертификатами и лотерейными билетами, денежными знаками и ценными бланками, валютными операциями, монетами и слитками из драгметаллов, кассовыми операциями. Так же к данным системам можно отнести веб-сайт ПАО «Сбербанк» и Сбербанк Бизнес Онлайн.

Процессинговые системы:

Процессинг – это процесс обработки данных, предусматриваемых при проведении платежных операций. Процессинговые центры, предоставляющие услуги по поставке программного обеспечения и обслуживания платежных систем, являются одним из звеньев системы эквайринга. Его цель – осуществление платежных транзакций по платежным картам.

Участниками эквайринговых операций являются:

1. Компания-эквайер, непосредственно осуществляющая расчет.
2. Банк-эмитент, который выпустил пластиковую карту.
3. Платежная система – посредник между предыдущими участниками.

Процессинговая система обязана обеспечить постоянную бесперебойную связь между участниками расчётов.

CRM система:

CRM-система или управление отношениями с клиентами - это прикладное программное обеспечение для организаций, предназначенное для автоматизации стратегий взаимодействия с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путем сохранения информации о клиентах и истории взаимоотношений с ними, установления и улучшения бизнес-процессов и последующего анализа ре-

зультатов. CRM-системой можно считать любой вариант контроля и учета, который поможет улучшить взаимодействие с клиентами.

BI-системы:

BI-системы – это аналитические системы, предназначенные для бизнес анализа, которые способны объединить данные из совершенно разных источников информации. Данные программные системы обрабатывают информацию, и предоставляют отчёт в удобном интерфейсе, для детального изучения и последующей оценки полученных в процессе сведений.

В ПАО «Сбербанк» существует Центр компетенции развития BI. По данным одного из выпусков корпоративной газеты для сотрудников ПАО «Сбербанк» Технологии, в ведении центра находятся: программно-аппаратный комплекс Teradata, включающий аналитическое хранилище данных, оперативное хранилище данных Oracle Exadata и еще одна система – витрины MIS.

Кредитные АС:

Необходимы для автоматизации операций кредитования физических лиц. Системы включают операции кредитования физических лиц, учет обеспечения по кредитам, учет резервов по кредитам, ведение части функционала позднего сбора по просроченной кредитной задолженности.

АС по управлению рисками:

Данные системы предназначена для автоматизированного управления рисками, помогают снизить операционные потери от реализации рисков и повысить инвестиционную привлекательность.

АС по управлению инвестициями:

АС данного типа предназначены для автоматизации функций первичного учета и сопровождения операций на фондовых рынках в рамках собственного порт-

феля центрального аппарата, портфелей территориальных банков и отделений банка в Москве, операций брокерского обслуживания и доверительного управления активами клиентов. Системы обеспечивают автоматизацию функций первичного учета и сопровождения казначейских операций центрального аппарата ПАО «Сбербанк» на денежных рынках и на рынках драгметаллов.

АС по управлению внутрихозяйственной деятельностью и персоналом:

Позволяет обеспечить единое информационное пространства для сквозных процессов по учету хозяйственных операций (с момента регистрации договора, до момента оплаты обязательств по договору), однократного ввода первичных документов с одновременным отражением необходимых данных в оперативном, бухгалтерском и налоговом учете. АС УВХД повышает эффективность деятельности Банка в части договорной работы, сокращает время и трудозатраты на обработку хозяйственных операций путем стандартизации и унификации процессов управления и учета, уменьшает трудоемкость при подготовке бухгалтерской, налоговой, управленческой и статистической отчетности в части ведения хозяйственной деятельности Банка.

АС платформы BPM:

BPM системы или системы управления бизнес-процессами - это класс корпоративных информационных систем, позволяющих автоматизировать процесс управления компанией и эффективностью бизнеса. BPM-системы осуществляют мониторинг, поиск несоответствий и возможностей улучшения процессов, происходящих в компании. При помощи BPM-систем отдел информационных технологий компании может моделировать существующие бизнес-процессы и вводить в действие новые.

АС, связанные с обслуживанием клиентов в удаленных каналах:

Данные системы являются базовыми инструментами для автоматизации всех процессов, связанных с сервисным обслуживанием поставляемых компанией продуктов и услуг. Системы позволяют существенно улучшить качество обслуживания клиентов и при этом сократить расходы на обслуживание за счет повышения эффективности работы сотрудников службы поддержки. К таким системам можно отнести Сбербанк Онлайн - самую популярную платформу в России для дистанционного получения банковских услуг.

1.4. Сервис онлайн-банкинга

Сервис онлайн-банкинга или Сбербанк Онлайн - это автоматизированная система обслуживания клиентов ПАО «Сбербанк» посредством сети Интернет. Система Сбербанк Онлайн дает возможность управлять своими картами и счетами, и производить платежные операции. Услуга была запущена в апреле 2008 года. Изначально пользователю был доступен достаточно узкий перечень возможностей - в первую очередь управление счетами, а также платежи и переводы. В то время сервис носил весьма консервативное название - «Электронная сберкасса» и не пользовался большой популярностью. Во многом это было связано с недоверием к электронным платежным системам со стороны консервативного большинства клиентов ПАО «Сбербанк», а затем с финансовым кризисом 2008-2009 годов. Но, по мере улучшения экономической ситуации, практических мер в рамках ребрендинга ПАО «Сбербанк», направленных на модернизацию его имиджа, и кратного роста числа пользователей онлайн-банкинга расширялся список возможностей, доступных клиентам банка. Сегодня это очень удобный сервис для управления финансами, который включает в себя множество разнообразных функций.

1.4.1. Назначения и преимущества

Для работы с системой Сбербанк Онлайн необходимо иметь банковскую карту ПАО «Сбербанк», подключенную к услуге Мобильный банк. Для входа в Сбербанк Онлайн необходимы идентификатор пользователя/логин и постоянный пароль. В качестве дополнительного подтверждения входа и подтверждения совершения операций используются одноразовые пароли, полученные в сообщениях на мобильный телефон. Срок действия одноразовых паролей ограничен.

Вход в Сбербанк Онлайн осуществляется через интернет браузер с любого устройства, либо через официальные мобильные приложения для смартфона.

Сбербанк Онлайн обеспечивает клиентам банка ряд преимуществ, в числе которых можно увидеть:

1. Возможность дистанционно пользоваться всеми продуктами банка.

2. Возможность управлять своими счетами и перечислять средства как внутри банка, так и за его пределы.

3. Экономию средств: переводы между собственными счетами и перечисления другим физическим лицам в пределах единой тарифной зоны осуществляются бесплатно.

4. Получение информационной поддержки в режиме 24/7.

5. Возможность приобретать банковские продукты на более выгодных условиях (к примеру, ставки по депозитам в системе всегда выше в сравнении с базовыми, доступными клиентам в отделениях).

1.4.2. Основные возможности

Ни для кого не секрет, что с развитием интернета и мобильных устройств связи возможности, ранее доступные только в отделениях банков, фактически переезжают в карман клиенту. Поэтому в современном мире финансов немаловажным критерием, влияющим на оценку (выбор) банковской организации, является предлагаемая ею система дистанционного обслуживания, а точнее набор возможно-

стей, предлагаемых этой системой. Рассмотрим, что же позволено клиентам ПАО «Сбербанк» онлайн-банкинг:

1. Выполнять операции с банковскими картами, а именно переводить деньги между своими карточными счетами и на счета третьего лица. Также есть возможность заблокировать карту и ознакомиться с выпиской.

2. Оформить вклады в рублях, долларах и евро на льготных условиях, пополнять или переводить средства с одного вклада на другой, получать выписки и прочее.

3. Подать заявку на получение кредита или кредитной карты.

4. Погашать кредиты ПАО «Сбербанк» с карты, вкладного или текущего счета.

5. Открыть обезличенный металлический счет и выполнять операции с банковскими металлами.

6. Подключить услугу автоматических платежей.

7. Получить выписку из Пенсионного фонда по своему лицевому счету.

8. Осуществлять платежи и обмен валют, оплачивать коммунальные услуги, мобильную связь, осуществлять платежи по произвольным реквизитам, переводить средства частному лицу-клиенту ПАО «Сбербанк» или другого российского банка.

9. Забронировать авиабилеты и оплатить их на сайте Аэрофлота.

1.4.3. Недостатки

Использовать Сбербанк Онлайн очень удобно, ведь клиентам предлагается огромный спектр функций. Каждый день всё больше людей начинает активно использовать данный сервис, а это в свою очередь приводит к большому интересу со стороны злоумышленников, которые могут украсть важную информацию, а в следствии и деньги клиентов. Отсюда вытекает основной недостаток онлайн-

банкинга, а именно: слабая защищенность интернет среды, в том числе и программ коммуникации, от несанкционированного доступа.

Для того чтобы быть в полной безопасности, необходимо придерживаться определенных мер защиты.

1.4.4. Меры безопасности по использованию сервиса

Для входа в систему Сбербанк Онлайн не требуется вводить никакой другой информации, кроме идентификатора/логина и пароля, а так же в некоторых случаях одноразового пароля. Если предлагается ввести любую другую персональную информацию или дополнительные данные (номер мобильного телефона, контрольную информацию по банковским картам или другие данные), это указывает на мошенничество. В таких случаях необходимо немедленно прекратить сеанс работы в системе Сбербанк Онлайн и срочно обратиться в банк.

При получении от банка СМС-сообщения с одноразовым паролем необходимо внимательно ознакомьтесь с информацией в сообщении: все реквизиты операции в направленном сообщении должны соответствовать той операции, которая совершается в данный момент. Пароль можно вводить только после тщательной проверки информации.

Вводя одноразовый СМС-пароль, клиент даёт банку право и указание провести операцию с указанными в СМС-сообщении реквизитами. Тем самым клиент ставит свою электронную подпись.

Ни при каких обстоятельствах нельзя сообщать пароли третьим лицам, включая работников банка.

При работе с сервисом Сбербанк Онлайн необходимо проверить, что установлено защищенное ssl-соединение с официальным сайтом сервиса (https://online.sberbank.ru). В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера. Например, в браузере Microsoft Internet Explorer версия 8.0 в правой

части адресной строки располагается желтый замочек, в более ранней версии – его изображение находится в правом нижнем углу экрана.

Для мобильных устройств существуют специально разработанные банком приложения. Рекомендуется использовать именно их, вместо мобильного интернет браузера.

Для исключения компрометации финансовой информации и хищения средств, настоятельно не рекомендуется подключать к услугам банка корпоративные номера телефонов и номера, которые не принадлежат клиенту, в том числе по рекомендации третьих лиц, представившихся работниками банка.

Нельзя устанавливать на мобильный телефон или иное устройство, на которое банк отправляет СМС-сообщения с подтверждающими одноразовыми паролями, приложения по ссылкам, полученным от неизвестных источников.

На смартфонах и иных устройствах, подключенных к сервису Сбербанк Онлайн, рекомендуется использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно.

На компьютерах, для работы в Сбербанк Онлайн рекомендуется:

1. Использовать современное антивирусное программное обеспечение и следить за его регулярным обновлением.

2. Своевременно устанавливать обновления операционной системы, рекомендуемые компанией-производителем.

3. Использовать дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ» - рассылок и прочего.

4. Завершать работу с системой путем выбора соответствующего пункта меню на сайте.

1.5. Основные способы защиты информации

К основным способам защиты информации можно отнести следующее:

1. Уникальные подписи и ключи, которые генерируются индивидуально для каждого клиента. Этот механизм чаще используется при обслуживании ПАО «Сбербанк» компаний, но иногда его предлагают и индивидуальным клиентам. Плюс ЭЦП в том, что она позволяет однозначно идентифицировать пользователя.

2. В сервисе Сбербанк Онлайн применяется SSL-шифрование данных, передаваемых от компьютера пользователя в систему банка и обратно. Эта мера безопасности позволяет исключить распространенный ранее вид мошенничества. Раньше часто использовалась схема «man in the middle»: данные о платеже перехватываются на этапе, когда они отправлены от клиента, но еще не дошли в банк. Злоумышленник меняет данные и только после этого отправляет их в банк. Чтобы воспользоваться всеми преимуществами защищенной передачи данных, следует соблюдать элементарные меры безопасности в интернете - не реагировать на подозрительные сообщения (полученные якобы от банка) и не переходить по неизвестным ссылкам.

3. Способ аутентификации пользователя посредством одноразовых паролей, создаваемых методом генерации случайных чисел. При такой системе каждая операция, которую совершает клиент с помощью сервиса, должна быть подтверждена одноразовым паролем, который приходит в виде СМС-сообщении на мобильный телефон. Такая система имеет ряд преимуществ. Во-первых, она достаточно проста в использовании - не нужно специальное оборудование, а процедура подтверждения операции занимает всего пару минут. Во-вторых, она позволяет обезопасить учетную запись от использования злоумышленниками - даже если известен логин и пароль для входа в систему.

4. Уведомления по СМС-сообщениям о том, что кто-то вошел в интернет-банк или проводит какую-то операцию позволяет клиенту заблаговременно узнать о несанкционированных операциях.

Помимо перечисленного выше, ПАО «Сбербанк» применяет дополнительные меры для обеспечения безопасного пользования онлайн-банкингом:

1. Ограничение использования личного сертификата - позволяет использовать электронный ключ (электронный сертификат) только на том компьютере, на котором он был сгенерирован. Таким образом, осуществлять платежи через онлайн-банкинг клиент сможет только со своего личного компьютера.

2. Виртуальная клавиатура – предназначена для того, чтобы злоумышленники не могли считать регистрационные данные при вводе их с обычной клавиатуры с помощью компьютерных вирусов.

3. Ограничение длительности сессии – в случае неактивности пользователя, сессия в системе онлайн-банкинга через определенное время (15 минут) будет закрыта. После этого для возобновления работы потребуется заново пройти аутентификацию.

4. История подключений – с помощью этой функции пользователь онлайн-банкинга узнает, если кто-то кроме него подключался к системе.

1.6. Нарушители информационной безопасности

Нарушитель - это злоумышленник, который осознано, по незнанию или по ошибке предпринял попытку выполнения запрещенных операций, использовав при этом различные возможности, методы и средства.

Его целью является получение контроля над информационным активом, приводящего к нарушению доступности, целостности или конфиденциальности.

Для предотвращения угроз, необходимо смоделировать действия нарушителя и ответную реакцию сервиса онлайн-банкинга. Это позволит произвести детальный анализ и предсказать поведение системы в определенных условиях.

В сервисе онлайн-банкинга можно выделить две группы нарушителей:

1. Нарушители, воздействующие на вычислительные системы банка, предоставляющие услуги СДБО (система дистанционного банковского обслуживания).

2. Нарушители, воздействующие на клиента СДБО (клиент, использующий сервис онлайн-банкинга).

В каждой группе можно выделить две категории нарушителей:

1. Организованные нарушители (группировки).

2. Одиночные нарушители.

Главной целью каждой категории нарушителей является незаконное получение денежных средств, путем использование вредоносного ПО.

Смоделируем первую группу нарушителей:

Категория нарушителей: организованные нарушители (группировки).

Состав организованной группы:

1. Организаторы, чьей задачей является руководство процессом незаконного получения денежных средств, выбор жертв и исполнителей, обеспечение безопасности).

2. Исполнители.

Исполнители делятся на соответствующие подкатегории:

1. Внутренние исполнители или инсайдеры - сотрудники банка, предоставляющие услуги СДБО. Их основной задачей является сбор данных о системе, использование известных уязвимостей, установка вредоносного ПО.

2. Консультанты - специалисты, обладающие определенными знаниями в технических и правовых областях. Их задачей является тактическое планирование и консультирование организаторов и инсайдеров.

3. Разработчики вредоносного ПО, задачей которых является создание специализированного ПО конкретно под атакуемый банк. Оно должно обеспечивать такие функции как выполнение заданных алгоритмов для хищения денежных средств, сокрытия следов преступления, нарушения работы ОС жертвы после вы-

полнения алгоритмов. ПО не должно детектироваться антивирусными программами, блокировать возможность обнаружения системными администраторами, минимизировать данные.

4. Специалисты по получению денежных средств, задачей которых является снятие денежных средств или перевод их на легальные счета.

Категория нарушителей: одиночные нарушители.

В данном случае будет отсутствовать внешний организатор , а консультант будет использоваться в качестве помощи. Такой нарушитель обладает высоким уровнем знаний в области IT, является специалистом. Для незаконного получения денежных средств он использует готовые программные решения.

Смоделируем вторую группу нарушителей:

Категория нарушителей: организованные нарушители (группировки).

Состав организованной группы:

1. Организаторы.

2. Исполнители.

Исполнители делятся на подкатегории:

1. Разведчики - специалисты по выявлению жертв. Они занимаются анализом и сбором данных, например, об используемом ПО и аппаратном обеспечении, использовании средств защиты (двухфакторная аутентификация).

2. Разработчики специализируемого ПО.

3. Распространили вредоносного ПО - специалисты по подготовке бот сетей и покупке или созданию зараженных данным ПО сайтам.

4. Специалисты по специальным вопросам, в обязанности которого входит преодоление системы защиты двухфакторной аутентификации, например, выпуском дубликата SIM карты с номером телефона, за которой закреплен онлайн-банкинг клиента. Сделать это можно путем подложных доверенностей или подделки временного удостоверения личности.

5. Специалисты по получению денежных средств.

Категория нарушителей: одиночные нарушители.

Может прибегать к информации расположенной на специализированных (закрытых) форумах и сайтах. Специалист разного уровня. Для незаконного получения денежных средств использует готовые программные решения.

1.7. Модель угроз и уязвимостей

Угроза безопасности - это намеренное нарушение безопасности, абсолютно любое событие или обстоятельство, которое может стать причиной нанесения ущерба защищаемому ресурсу банка.

Источники угроз являются главными носителями угроз безопасности информации в банке. Они могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Источники угроз могут быть разделены на:

1. Человеческие, когда действия или бездействие физического лица несут прямую угрозу нанесения ущерба. Человеческие угрозы исходят от внешних и(или) внутренних нарушителей информационной безопасности и подразделяются на:

1. Преднамеренные - компьютерные атаки, взломы, несанкционированная модификация электронной информации.

2. Непреднамеренные - ошибки при проектировании и разработке ПО, ошибки при эксплуатации информационных систем.

2. Технические, возникающие в результате самопроизвольного выхода из строя того или иного электронного оборудования. К ним относятся технические

сбои и отказы оборудования СДБО. Например, выход из строя серверов или компьютеров, каналов связи по причине заводского брака оборудования, несовместимости версий ПО.

3. Непредвиденные обстоятельства - стихийные бедствия, аварии, пожары, наводнения, землетрясения, ураганы, массовые беспорядки.

В таблице 1 представлены угрозы и уязвимости сервиса Сбербанк Онлайн.

Таблица 1 - Угрозы и уязвимости

Угроза	Уязвимость
1	2
1. Авторизация пользователя через СМС-сообщения.	Возможность перехватить СМС-сообщения через: 1. Специальное оборудование, так как передача идёт по незащищенному каналу. 2. Заражение мобильного телефона вирусами или вредоносным ПО.
2. Аутентификация пользователя.	Отсутствуют эффективные методы по однозначному определению клиента

Продолжение таблицы 1

1	2
3. Подтверждения действий клиента через СМС-сообщения.	Возможность перехватить СМС-сообщения через: 1. Специальное оборудование, так как передача идёт по незащищенному каналу. 2. Заражение мобильного телефона вирусами или вредоносным ПО.
4. Плохая осведомленность клиентов по вопросам безопасности. Цифровая грамотность пользователей очень низкая.	Отсутствует обязательное тестирование на знание безопасности.

1.8. Расчёт рисков

Сначала рассчитываем уровень угрозы по уязвимости Th на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

где ER - критичность реализации угрозы (указывается в %),

а P(V) - вероятность реализации угрозы через данную уязвимость (указывается в %).

Вычисляем одно или три значения в зависимости от количества базовых угроз. Получаем значение уровня угрозы по уязвимости в интервале от 0 до 1.

Чтобы рассчитать уровень угрозы по всем уязвимостям CTh, через которые возможна реализация данной угрозы на ресурсе, просуммируем полученные уровни угроз через конкретные уязвимости по следующей формуле:

Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th)$$

Значения уровня угрозы по всем уязвимостям получим в интервале от 0 до 1.

Аналогично рассчитываем общий уровень угроз по ресурсу CThR (учитывая все угрозы, действующие на ресурс):

Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh)$$

Значение общего уровня угрозы получим в интервале от 0 до 1.

Таблица 2 - Расчёт рисков

У-У	P(V) %	ER %	Th	CTh	CThR
1.1	70	95	0.67	0.8581	0.995
1.2	60	95	0.57		

2	60	90	0.54	0.54
3.1	70	95	0.67	0.8581
3.2	60	95	0.57	
4	60	70	0.42	0.42

Из расчетов видно, что основными уязвимостями являются:

Возможность перехватить СМС-сообщения через специальное оборудование, так как передача идёт по незащищенному каналу или через заражение мобильного телефона вирусами или вредоносным ПО.

Отсюда можно сказать, что меры для понижения рисков в первую очередь надо направить на эти уязвимости.

ГЛАВА 2. МЕРЫ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОНЛАЙН-БАНКИНГА

2.1. Меры по повышению эффективности защиты

С каждым годом количество киберпреступлений в сервисах онлайн-банкинга растёт. Предполагается, что потенциальный Злоумышленник обладает высокой квалификацией, знаниями в IT-сфере, программно-аппаратными средствами реализации атаки. В связи с этим возникает необходимость постоянного анализа систем на появление новых уязвимостей и угроз.

Злоумышленники могут проводить несанкционированные транзакции или получать полный контроль над сервисом онлайн-банкинга, в случае если сервис будет иметь серьезные недостатки механизмов аутентификации, авторизации и системы подтверждения действий клиента. Такие инциденты могут привести к существенным финансовым потерям и подпортить репутацию банка.

По ходу анализа сервиса Сбербанк Онлайн была выявлена очень важная уязвимость - использование СМС-сообщений как способа подтверждения. По мимо этого мною были разработаны эффективные меры по повышению защиты сервиса Сбербанк Онлайн.

2.1.1. СМС-сообщения

СМС-сообщения, в которых приходят одноразовые пароли для авторизации или подтверждения действий клиента, являются уязвимостью сервиса Сбербанк

Онлайн. Данный метод используют почти во всех сервисах схожего типа, но является небезопасным.

Основная уязвимость хранится именно в незащищенности передачи СМС-сообщения, ведь оно приходит клиенту прямо на экран мобильного телефона по незащищенному каналу. Злоумышленники могут перехватить такое сообщение с помощью специального оборудование или вредоносного ПО, заранее установленного на смартфон жертвы.

По мимо перехвата данной информации, можно использовать лазейки в законодательстве РФ. Например, узнав номер мобильного телефона жертвы, злоумышленник может восстановить сим карту в любом салоне связи оператора за считанные минуты. Для этого ему потребуется поддельный документ о временном удостоверении личности, который можно с легкостью купить на черном рынке интернета. Далее исход очевиден - восстанавливается логин и пароль от сервиса онлайн-банка посредством СМС-сообщения, выполняется авторизация по новым данным и осуществляется перевод денег со счёта клиента на счета злоумышленника. В случае если у злоумышленника есть знакомые люди в операторах сотовой связи, подделать сим карту они смогут без каких-либо документов и подтверждений.

Исключить СМС-сообщения из сервиса онлайн-банкинга полностью сегодня нельзя, т.к. ещё нет более простых и эффективных способов подтверждения, но их можно заменить на более эффективные методы. Предлагается использование одноразовых паролей, выдаваемых в банкомате на чеке, например, в количестве 25 штук. Злоумышленники действуют в основном только в онлайн сфере, потому что так их сложно найти и вычислить, поэтому красть данный чеки у клиентов банка будет неразумным и опасным решением.

Может оказаться так, что поблизости нет банкоматов, а одноразовые пароли нужны. В этом случае предлагается использовать специальный выделенный номер телефона с автоответчиком, который будет подтверждать операции. Допустим, если клиент хочет сделать перевод, ему будет предложено позвонить на спе-

циальный номер, прослушать информацию о переводе, а затем ввести USSD запрос о подтверждении.

2.1.2. Двухфакторная авторизация в мобильных приложениях

В мобильных приложениях отсутствует двухфакторная авторизация клиента. При входе в онлайн банк используется система биометрических данных - отпечаток пальца. В случае, если мобильный телефон не поддерживает данную функцию, предлагается использовать заранее придуманный пароль. Данный метод будет эффективные, если в связке с этим будут использоваться одноразовые коды подтверждения, полученные предварительно в банкомате.

Если поблизости нет банкомата, то клиенту будет предложен вариант звонка в банке на специальный номер телефона и подтвердить своё действие USSD командой.

2.1.3. Подтверждение новых устройств

Сейчас в сервисе онлайн-банкинга клиент может зарегистрировать неограниченное количество устройств. Это является небезопасным методом, так как злоумышленники смогут добавить новое устройство и при желании осуществить вход в сервис.

Идея подтверждения новых устройств заключается в том, что при регистрации карты и подключения услуги Сбербанк Онлайн, клиенту будет предложено количество устройств, которые он собирается использовать. Например, у клиента есть компьютер, планшет и мобильный телефон. Сбербанк Онлайн будет использоваться на каждом из устройств. В этом случае клиент укажет возможность добавить только три новых устройства и будет обязан подключить каждое из них в течение определенного времени. Если злоумышленник будет пытаться добавить но-

вое устройство, ему будет отказано в доступе, так как количество добавленных устройств будет превышено.

В случае, если клиенту необходимо зайти в Сбербанк Онлайн с рабочего места или от друзей, будет существовать такой вариант как временная сессия. Смысл её будет заключаться во временной регистрации нового устройства, например, на 15 минут. После чего сеанс с сервисом Сбербанк Онлайн будет прекращен. Для подтверждения новой сессии, предлагается использовать подтверждение по специально выделенному номеру банка, куда клиент должен будет позвонить и подтвердить своё действие через USSD запрос. В данном случае перехват информации со стороны злоумышленника будет почти невозможен, а действовать в оффлайне абсолютно неразумным и очень затратным.

2.1.4. Местоположение клиента

Сервис Сбербанк Онлайн не имеет такой важной функции как запись местоположения клиента. Данная функция могла бы сыграть очень значимую роль в обеспечении безопасности сервиса онлайн-банкинга.

Идея данного метода заключатся в ограничение использование сервиса за пределами другого города и страны. В настройках сервиса появится соответствующая настройка, которая будет позволять клиенту выбрать зону действия сервиса.

Если клиент выедет из области действий работы сервиса, все последующие операции необходимо будет подтвердить через звонок на специальный номер банка. Данный метод будет эффективен, так как злоумышленники не будут знать о зоне действий работы сервиса, а в случае несанкционированного списание денег, будет произведена блокировка из-за невозможности подтвердить операцию.

2.1.5. Однозначное определение пользователя

Идея однозначного определения пользователя заключатся в том, что каждые действия клиента будет анализировать робот и записывать их в соответствующие разделы. В качестве исследований можно использовать такие параметры как IP адрес, MAC адрес, устройство, браузер или мобильное приложение под конкретную операционную систему, скорость ввода одноразовых паролей или скорость звонка в банк, время входов в сервис онлайн-банкинга, частота входа в сервис в день и прочее. По данным параметрам можно будет составить модель поведения клиента в сервисе, что позволить блокировать несанкционированный доступ со стороны злоумышленников. В случае, если система сработает неверно и заблокирует клиента, будет доступен способ разблокировки сервиса посредством одноразовых паролей или звонку в банк.

2.1.6. Онлайн тестирование

Сегодня, цифровая грамотность населения пользователей онлайн-банкинга очень низкая. При регистрации в сервисе, многие клиенты просто соглашаются с правилами, даже не прочитав их.

Идея онлайн тестирования, заключается в проведении обязательного тестирования со стороны банка, например, если клиент оформляет карту через сайт, после успешного заполнения заявки, будет предложено пройти небольшое тестирование на знание сервиса и на соблюдение требований безопасности. В случае, если клиент открывает карту прямо в офисе ПАО «Сбербанк», пройти тестирование можно будет посредством SMS, банкоматов, либо компьютеров в офисе банка.

Данное обязательное онлайн тестирование поможет повысить цифровую грамотность населения, в следствии чего клиенты будут лучше осведомлены по вопросам безопасности использования онлайн-банкига.

ГЛАВА 3. АНАЛИЗ ЭФФЕКТИВНОСТИ ЗАЩИТЫ СЕРВИСА ОНЛАЙН-БАНКИНГА ПОСЛЕ ВНЕДРЕНИЯ МЕР ПО ПОВЫШЕНИЮ БЕЗОПАСНОСТИ

3.1. Расчёт рисков ИБ после модернизации системы защиты

После модернизации системы защиты сервиса онлайн-банкинга Сбербанк Онлайн, произведем расчёт рисков информационной безопасности по новым показателям ERи P(V), которые были рассчитаны и получены от экспертной группы аналитиков информационной безопасности ПАО «Сбербанк».

Угрозы и уязвимости возьмём из ГЛАВЫ 1 пункта 1.7.

3.1.1. Входные данные

Таблица 3 - Входные данные 1

Ресурс	Угрозы	Уязвимости
1	2	3
Сервис онлайн-банкинг (критичность ресурса - 100 у.е).	Угроза 1 Авторизация пользователя через СМС-сообщения.	Уязвимость 1 Возможность перехватить СМС-сообщения через специальное оборудование, так как передача идёт по незащищенному каналу.
		Уязвимость 2 Возможность перехватить СМС-сообщения через заражение мобильного телефона вирусами или вредоносным ПО.

Продолжение таблицы 3

1	2	3
Сервис онлайн-банкинг (критичность ресурса - 100 у.е).	Угроза 2 Аутентификация пользователя.	Уязвимость 1 Отсутствуют эффективные методы по однозначному определению клиента.
	Угроза 3 Подтверждения действий клиента через СМС-сообщения.	Уязвимость 1 Возможность перехватить СМС-сообщения через специальное оборудование, так как передача идёт по незащищенному каналу.
		Уязвимость 2 Возможность перехватить СМС-сообщения через заражение мобильного телефона вирусами или вредоносным ПО.
	Угроза 4 Плохая осведомленность клиентов по вопросам безопасности. Цифровая грамотность пользователей очень низкая.	Уязвимость 1 Отсутствует обязательное тестирование на знание безопасности.

Таблица 4 - Входные данные 2

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через уязвимость (%), ER
Угроза 1/Уязвимость 1	30	50
Угроза 1/Уязвимость 2	20	50
Угроза 2/Уязвимость 1	20	40
Угроза 3/Уязвимость 1	30	50
Угроза 3/Уязвимость 2	20	50
Угроза 4/Уязвимость 1	50	60

3.1.2. Уровень угрозы

Таблица 5 - Уровень угрозы

Угроза/Уязвимость	Уровень угрозы (%), Th $Th = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$
Угроза 1/Уязвимость 1	0.15	0.235
Угроза 1/Уязвимость 2	0.10	
Угроза 2/Уязвимость 1	0.08	0.08
Угроза 3/Уязвимость 1	0.15	0.235
Угроза 3/Уязвимость 2	0.10	
Угроза 4/Уязвимость 1	0.30	0.30

3.1.3. Общий уровень угроз, действующих на ресурс

Таблица 6 - Общий уровень угроз

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$	Общий уровень угроз по ресурсу (%), CThR $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$
Угроза 1/Уязвимость 1	0.235	0.625
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1	0.08	
Угроза 3/Уязвимость 1	0.235	
Угроза 3/Уязвимость 2		
Угроза 4/Уязвимость 1	0.30	

3.1.4. Риск ресурса

Критичность ресурса (ущерб, который понесет банк от потери ресурса) - 100 у.е. Для угрозы доступность, критичность ресурса задается в час (а не в год, как для остальных угроз). Поэтому, чтобы получить критичность ресурса в год, необ-

ходимо умножить критичность ресурса в час на максимально критичное время простоя ресурса за год.

Таблица 7 - Риск ресурса

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), CThR $CThR = 1 - \prod_{i=1}^{n}(1 - CTh)$	Риск ресурса (у.е.), R R = CThR x D
Угроза 1/Уязвимость 1	0.625	62.5
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		
Угроза 4/Уязвимость 1		

3.1.5. Оценка эффективности после модернизации ИБ онлайн-банкинга

До модернизации системы защиты онлайн-банкина, общий уровень угроз, действующий на ресурс был равен 0.995 , а после модернизации стал 0.625. Отсюда видно, что данный показатель уменьшился примерно в полтора раза, что говорит об успешной проведении работы. Уровень угроз по основным уязвимостям был значительно снижен. Это видно из показателей CTh до и после.

Уровень таких уязвимостей как перехват СМС-сообщения через специальное оборудование или через заражение мобильного телефона вирусами или вредоносным ПО стал значительно ниже.

Так, после внедрения специальных мер по улучшение защиты информации сервиса онлайн-банкинга, можно с уверенностью сказать что защита стала эффективней. Данные выводы сделаны опираясь на расчеты рисков до и после.

ЗАКЛЮЧЕНИЕ

В ходе данной работы сервис онлайн-банкинга Сбербанк Онлайн был проанализирован на угрозы и уязвимости, были произведены расчёты рисков. После анализа были предложены меры для повышения эффективности систем защиты от несанкционированного доступа. Данные меры значительно повысили надежность и безопасность сервиса Сбербанк Онлайн. Данные выводы сделаны по второму анализу, который был произведен после предложенных мер. Так, например, показатель общего уровня угроз, действующих на ресурс снизился почти в полтора раза, а показатели уровня угроз по каждой уязвимости в два раза. Данные результаты можно посчитать идеальными, так как достигнутая цель работы была достигнута.

ПРИЛОЖЕНИЕ А

Core banking:

1. АС ЦОД (автоматизированная система централизованного обслуживания вкладов физических лиц).

2. АС BackOffice (централизованная база депозитов физлиц).

3. АС УПД (управление платежными документами).

Данные системы предназначены для обслуживания розничного сектора клиентов ПАО «Сбербанк» и ориентированы, в первую очередь, на обслуживание физических лиц. В числе операций, которые выполняются с их помощью – обеспечение хранения счетов по вкладам физических лиц и данных о клиентах, обслуживание запросов структурных подразделений отделений о состоянии счетов по вкладам физических лиц, прием банковских транзакций от функциональных подсистем операционного уровня и др.

4. АС Юпитер (хранение и обработка информации по зарплатным проектам).

5. Корпоративная АБС автоматизации операций клиентов (юридических лиц и физических лиц, являющихся собственниками бизнеса).

6. АС ГАММА (формирование бухгалтерских проводок на основании реестров сделок и платежных документов).

7. АС Кассовый центр (решение, автоматизирующее процессы кассовых узлов и кассово-инкассаторских центров).

8. АС Виват (система по учету и ведению военных пенсий).

9. АС ТФиДО (глобальная платформа сопровождения торгового финансирования и документарных операций).

10. АС Централизованная автоматизированная система ведения нормативно-справочной информации.

Системы FrontEnd:

Одной из центральных систем данного блока является АС ФС, позволяющая выполнять функции администрирования офисом, приема платежей и переводов, погашения кредита физических лиц, работы со счетами и вкладами, банковскими картами, сберегательными сертификатами и лотерейными билетами, денежными знаками и ценными бланками, валютными операциями, монетами и слитками из драгметаллов, кассовыми операциями.

Также к FrontEnd системам относятся:

1. АС xBank (система банка, используемая для автоматизации работы операционных и кассовых работников в ВСП по вводу и обработке большинства операций розничного блока).

2. АС Инфобанк (система для автоматизации операций по ценным бумагам ПАО «Сбербанк», дорожным чекам иностранных эмитентов, ведения централизованного реестра проблемных ценных бумаг).

3. АС Сбор данных (сбор данных по кредитным обязательствам).

4. АС Стоп-лист (ведение СТОП-ЛИСТов (террористы, недействительные документы, недобросовестные ссудозаёмщики), формирование транспортных файлов с реквизитами юридических и физических лиц, загрузка файлов журнала обращений и несоответствий).

5. АС ВИК Договоры (ведение информации по договорам клиентов и базы данных юридических лиц, заключивших с ПАО «Сбербанк» договор о зачислении денежных средств на счета физических лиц).

6. АС Банковское страхование, предназначенная для учета заявлений клиентов физических лиц по страхованию.

7. Веб-сайт ПАО «Сбербанк».

8. АС Dealing Manager (фронт-офисная система ведения позиции по сделкам на валютном, денежном и рынке драгметаллов).

9. АС КВРБ (компенсации вкладчикам разорившихся банков).

10. АС СББОЛ (СберБанкБизнесОнЛайн, предназначена для дистанционного управление счетами корпоративных клиентов посредством интернет браузера).

11. АС Сбербанк Корпорация (внедрение комплексных продуктов по управлению финансовыми потоками крупнейших, крупных и средних клиентов банка).

12. АС ЕФС (Единая Фронтальная Система), которая включает в себя всю фронтальную функциональность, связанную с автоматизацией обслуживания клиентов во всех каналах обслуживания и позволяет осуществлять кросс-канальные операции.

13. АС Клиент Сбербанк, обеспечивающая электронный документооборот и удаленное управление счетами для клиентов - юридических лиц ПАО «Сбербанк» в Москве. Обслуживает порядка 300 000 клиентов (70 инсталляций).

Процессинговые системы:

1. АС WAY4 (процессинговая система банковских карт).

2. АС SmartVista (фронтальная система, обеспечивающая онлайновое обслуживание авторизационных запросов по банковским картам и онлайновое взаимодействие с международными, и российскими платежными системами).

3. АС ЕРКЦ (единый распределенный контактный центр ПАО «Сбербанк» на платформе Avaya для автоматизации справочно-информационного обслуживания, телемаркетинга, службы помощи банка).

4. АС Запрос (шлюз запросов к внешним источникам информации).

5. АС Masspay (система приема платежей, предназначенная для построения сети приема платежей населения с использованием устройств самообслуживания (банкоматы, информационные киоски).

6. АС UPOS (универсальное ПО POS-терминалов и интегрированных кассовых решений в торгово-сервисных предприятиях эквайринговой сети Сбербанка).

7. АС СПООБК2 (система предварительной обработки операций по банковским картам второго поколения). Обеспечивает предварительную обработку операций с кредитными картами. Автоматизация процессов, обеспечивающих подготовку и предварительную обработку операций по кредитным картам для последующей передачи данных в программно-аппаратный комплекс WAY4.

8. АПК Matching - автоматизированная система, обеспечивающая формирование информации для проведения расчетов по банковским картам платежной системы MasterCard (карты, выпущенные сторонними банками), а также обеспечивающая формирование статистических и бухгалтерских отчетов.

9. АС IQWAVE (Шлюз Платежных Транзакций). Для упрощения создания, внедрения и сопровождения интеграционных взаимодействий между автоматизированными системами ПАО «Сбербанк» и поставщиками услуг.

10. АС ОПП (Обработка прямого потока). Предназначена для обработки файлов с информацией по выпуску/перевыпуску банковских карт, а также файлов с операциями пополнения/списания денежных средств по банковским картам.

11. АС Дебаты 2.0. Система предназначена для ведения претензионной работы по банковским картам, включая проверку изменения статуса урегулирования претензии, наличия зарегистрированной претензии и регистрации претензии.

12. АС СНУиЛ (система номерного учёта и логистики банковских карт и сопутствующих компонентов (Octopus). Обеспечивает мониторинг состояния всех видов банковских карт, учитывает количество израсходованных заготовок при производстве карты.

13. Сценарии устройств самообслуживания (Сценарий УС) - сценарии работы устройства самообслуживания с центральной фронтальной системой для

осуществления базовых клиентских операций с устройством – авторизации, выдачи и взноса наличных, работа с личным кабинетом, платежи и т.д..

14. ЕГПО (единое гибридное программное обеспечение, ПО устройств самообслуживания).

CRM:

1. АС CRM Розничный (система управления взаимоотношениями с клиентами розничного блока). В основе системы использован продукт Oracle Siebel CRM.

2. АС CRM Корпоративный (система управление взаимоотношениями с корпоративными клиентами). Автоматизирует такие функции как создание единого представления о клиенте, управление сотрудничеством с клиентом, закрепление клиента за ответственным подразделением/сотрудником, разграничение доступа к клиентской информации.

3. АС CRM Трансграничный (система управление взаимоотношениями с корпоративными клиентами банка, предназначена для автоматизации операций по работе с зарубежными корпоративными клиентами).

4. АС MDM Клиентский (система на базе MDM для построения единого профиля клиента физического и юридического лица). Реализация на IBM InfoSphere MDM Server.

5. АС MDM Продуктовый (централизованный каталог продуктов и тарифов). Реализация на IBM InfoSphere MDM Collaboration Server (бывший MDM Server for Product Information Management).

6. АС ФКД (формирование кредитной документации). Осуществляет обеспечение достоверности и актуальности шаблонов кредитных документов.

7. АС СУДИР (система управления доступом к информационным ресурсам).

8. АС ФО Клиентов (финансовая отчетность клиентов). Информация из системы используется для формирования блоков кредитной заявки, приложений к кредитной заявке, блоков форм мониторинга, а также аналитической отчетности.

9. АС Курсы валют (автоматизированная система установления валютных курсов и курсов драгоценных металлов по системе ПАО «Сбербанк»).

10. АС GoldenSource (Котировки финансовых инструментов (КФИ)) источник мастер-котировок для финансовых целей.

11. АС ЦАС ОК (Централизованная автоматизированная система Обращения клиентов) предназначена для регистрации обращений клиентов, классификации обращений, их обработки с возможностью передачи на экспертизу, подготовки и отправки ответа клиенту.

12. АС MIS обеспечивает руководство банка аналитической информацией для принятия управленческих решений.

BI-системы:

В ПАО «Сбербанк» существует Центр компетенции развития BI. По данным одного из выпусков корпоративной газеты для сотрудников «Сбербанк Технологии», в ведении центра находятся: программно-аппаратный комплекс Teradata, включающий аналитическое хранилище данных, оперативное хранилище данных Oracle Exadata и еще одна система – витрины MIS.

Кредитные АС:

1. АБС для автоматизации операций кредитования физических лиц. Система включает операции кредитования физических лиц, учет обеспечения по кредитам, учет резервов по кредитам, ведение части функционала позднего сбора по просроченной кредитной задолженности.

2. АС Transact SM Розничный (автоматизация предкредитной обработки по физическим лицам). Система предназначена для ведения, хранения и обновления информации о кредитных продуктах, а также для решения задач документооборота и принятия решения по заявкам клиентов физических лиц микросегмента малого бизнеса.

3. АС Transact SM СМП (предкредитная обработка заявок по кредитованию собственников малого бизнеса). Система предназначена для ведения, хранения и обновления информации о кредитных продуктах, а также для решения задач документооборота и принятия решения по заявкам клиентов микросегмента малого бизнеса.

4. АС Transact SM Экспресс-кредиты (система, позволяющая вводить, обрабатывать, хранить и выполнять поиск информации о клиентах и заявках на кредит в централизованной базе данных).

5. АС Централизованная ИАС Кредитование юридических лиц (централизованное ведение вкладов физических лиц с проведением централизованных зачислений и обеспечением межфилиальных операций). Система используется для проведения операций по счетам физических лиц, содержит актуальные остатки по счетам физических лиц.

6. АС Централизованная ИАС Кредитования физических лиц (обслуживание кредитных договоров физических лиц (фронт, мидл и бэк офис). Помимо потребительских, авто и ипотечных кредитов в системе также обслуживаются разрешенные овердрафты карточных счетов.

7. АС Tallyman (система для сбора просроченной задолженности).

8. АС Hunter (предупреждения о мошенничестве при рассмотрении кредитных заявок). Система проводит сравнение данных по вновь оформляемой кредитной заявке с уже имеющимися заявками с целью определения и предупреждения мошенничества.

9. АС ОКИ (система для оценки кредитных историй).

10. АС Калита (сбор просроченной задолженности физических лиц и малого-микро бизнеса). Данная система может взаимодействовать с внешними системами с целью информирования должника о наличии просроченной задолженности с использованием различных каналов; с системами госорганов (ФССП) для реализации судебного и исполнительного производства, с коллекторскими агентствами при передаче на сопровождение/продаже просроченного портфеля и др.

АС по управлению рисками:

1. Аналитический модуль расчета лимитов и рейтингов (АМРЛиРТ) - рейтинговая модель оценки вероятности дефолта контрагента. Рассчитывает вероятность дефолта и рейтинг заемщика, ожидаемые потери при дефолте заёмщика, кредитоёмкость, внутренний рейтинг.

2. АС СУОР (Система управления операционными рисками) - учет анализ, управление операционными рисками, своевременное выявление потенциальных угроз, снижения потерь при реализации операционных рисков.

3. СУККР (система управления корпоративными кредитными рисками). Предназначена для управление рисками корпоративного кредитного портфеля для решения таких бизнес-задач как прогноз уровня кредитных рисков с формированием и поддержкой базы данных по реализованным кредитным рискам, оценка рисков совокупного кредитного портфеля банка, контроль качества кредитного портфеля банка, проведение стресс-тестирования кредитного портфеля банка и др.

4. Автоматизированная система поведенческого скоринга для работы с просроченной задолженностью. Обеспечивает снижение расходов на мероприятия, связанные с взысканиями задолженности за счет проведения анализа поведенческих, статических и социально-демографических характеристик клиентов и учета результатов этого анализа при определении стратегии взыскания.

5. Система контроля качества андеррайтинга (СККА). Обеспечивает сбор и анализ информации о работе андеррайтеров банка, внутренний аудит качества работы кредитных подразделений.

6. Обеспечение гибкого механизма управления структурой лимитов риска, в т.ч. при условии дальнейшего усложнения методологии Автоматический расчет сумм лимитов различных типов в зависимости от факторов, определенных методологией банка.

7. SAP Bank Analyzer Limit Manager. Обеспечивает гибкий механизм управления структурой лимитов риска, расчет сумм лимитов различных типов и др.

8. АС Казначейство (комплексная автоматизированная система казначейства на единой платформе).

АС по управлению инвестициями:

1. АС DiasoftCUSTODY 5NT. Система предназначена для автоматизации функций первичного учета и сопровождения операций на фондовых рынках в рамках собственного портфеля центрального аппарата, портфелей территориальных банков и отделений банка в Москве, операций брокерского обслуживания и доверительного управления активами клиентов.

2. АС DiasoftDEALING 5NT. Система обеспечивает автоматизацию функций первичного учета и сопровождения казначейских операций центрального аппарата ПАО «Сбербанк» на денежных рынках и на рынках драгметаллов.

3. АС Дивиденд. Предназначена для бухгалтерского учета процесса выплаты дивидендов.

4. АС Реестр акционеров (ведение реестра акционеров ПАО «Сбербанк», проведение собрания акционеров).

5. АИС Депозитарий 2000. Система обеспечивает автоматизацию депозитария в части учета выпусков ценных бумаг, проведения бухгалтерских операций с ценными бумагами; хранение информации об эмитентах ценных бумаг и депонентах и др.

6. АС Murex (консолидированный риск трейдинга, P&L - консолидированный риск трейдинга и P&L - фронт-офис).

7. АС QUIK (система электронной торговли для клиентов брокерского обслуживания). Предоставляет доступ клиентам к торговле на фондовом, денежном и срочных рынках через веб или полноценный клиент;

8. АС ЦБДБО (централизованная база договоров брокерского обслуживания).

9. АС FX&MM Plus - занесение заявок корпоративных клиентов на размещение денежных средств в депозиты, векселя, сделок бронирования, а также привлечение кредитов, требующих согласования с департаментом казначейских операций и финансовых рынков, установления процентной ставки, акцептования, хранения и анализа информации по всем заявкам и сделкам с корпоративными клиентами, а также операций на валютном рынке.

10. АС eFX (стратегическая мультипродуктовая система электронной торговли Apama).

11. АС Фокус (фронт-офисная система казначейства на фондовом рынке, брокерское обслуживание клиентов на фондовом рынке).

12. АС SavEx – (электронная площадка для проведения торговых операций с внутренними подразделениями (территориальными банками ПАО «Сбербанк» и отделениями Москвы) и внешними клиентами.

13. АСУ ОВП (автоматизированная система управления открытой валютной позицией).

14. АС Calypso (TDS) - система продуктового учета внебиржевых деривативов.

15. АС Удаленное рабочее место депонента (ЛУЧ) - рабочее место для обеспечения электронного документооборота с «Национальным Депозитарным Центром» для исполнения поручений ПАО «Сбербанк» на ММВБ.

АС по управлению внутрихозяйственной деятельностью и персоналом:

1. Единая АС управления персоналом на базе SAP HCM.

2. Управление внутрихозяйственной деятельностью на базе SAP ERP.

3. АС платформы BPM.

4. АС Прометей (система управления процессами по обслуживанию зарплатных проектов). Система реализует задачи, связанные с управлением бизнес процессами: обработка заявки на заключение зарплатного договора, обработка карточки зарплатного договора, обработка электронного реестра, открытие счетов и выпуск карт и др.

5. АС ОАД (оперативный архив документов). Предназначена для автоматизации бизнес-процессов банка в части организации регистрации, учета размещения, контроля поступления и перемещения, поиска досье клиентов на бумажных носителях, а также для создания и хранения электронных образов документов досье клиентов банка на бумажных носителях.

6. АС Безбумажный Бэк-Миддл офис на базе BPM системы PegaRULES Process Commander (АС ББМО). Система автоматизирует и унифицирует работу по сканированию, передаче и обработке отсканированных копий бумажных документов с целью сокращения транспортных расходов. Реализовывает обработку поступающих от клиентов по системам ДБО документов в соответствии с утвержденными бизнес процессами.

7. АС ККМБ (кредитный конвейер малого бизнеса). Система построена на платформе PegaRULES Process Commander.

8. АС ЭДО с госорганами. Система включает функциональные подсистемы, каждая из которых реализует документооборот с определенным государственным учреждением.

9. АС ДИС (диспетчеризация кредитных заявок).

10. Система управления знаниями (АС СУЗ).

АС, связанные с обслуживанием клиентов в удаленных каналах:

1. ЕРИБ (единый розничный интернет-банк).

2. МБК (мобильный банк по картам). Обеспечивает предоставление информационных услуг держателям международных карт ПАО «Сбербанк» на мобильные телефоны.

3. МБВ (мобильный банк по вкладам). Обеспечивает информирование клиентов и совершение операций по оплате услуг со счетов вкладов с помощью SMS.

4. ЕРМБ – единый розничный мобильный банк (приложение Мобильный банк/Сбербанк Онлайн). Обеспечивает взаимодействие с клиентом банка посредством приема и отправки SMS-сообщений, USSD-запросов и PUSH-уведомлений для информирования клиентов о совершенных операциях и совершения активных операций по счетам и картам клиента;

5. АС СИРИУС (система интеграции устройств самообслуживания). Обеспечивает централизованное формирование сценариев взаимодействия устройства самообслуживания с клиентом; управление спецификацией предоставляемого клиенту набора бизнес-сервисов, доставку бизнес-сервисов до устройства самообслуживания.

6. АС Автоплатежи (предоставление клиентам банка услуги автоматических безналичных платежей со счетов банковских карт в адрес операторов сотовой связи.

7. АС Сверка (сверка операций на устройствах самообслуживания).

8. АС СМСУО - система мониторинга работы систем, управляющих очередями клиентов в подразделениях банка (электронная очередь). Построение централизованной отчетности по данным, поставляемым системами управления очередями.

9. АС ЕПС (единая платежная система). Предназначена для автоматизации работ по обработке принятых платежей от населения в филиалах (операционных частях) ПАО «Сбербанк», подготовке необходимых проверочных ведомостей, подготовке платежных поручений для перечисления сумм принятых платежей и подготовке электронных и бумажных реестров принятых платежей для организаций-получателей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Безмалый В. Защита интернет-банкинга // Windows IT Pro/RE. 2012.

2. Быстрова Е.Н., Сараев А.А. Интернет-бан- кинг в России: тенденции и перспективы развития // Новый университет. Сер. Экономика и право. 2013.

3. Закиров М.Р. Исследование угроз нарушения безопасности в системах дистанционного банковско- го обслуживания // Информационное противодейс- твие угрозам терроризма. 2014.

4. http://www.sberbank.ru/

5. http://www.tadviser.ru/index.php/

6. http://www.sberbank.ru/common/img/uploaded/files/pdf/UDBO.pdf#6

7. http://www.dsec.ru/