МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

Базовая кафедра современного банковского дела

Апалькова Анна Юрьевна

ЭФФЕКТИВНЫЕ МОДЕЛИ И СИСТЕМЫ ЗАЩИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ: ВОЗМОЖНОСТИ И УСЛОВИЯ ПРИМЕНЕНИЯ НА ПРИМЕРЕ ПАО СБЕРБАНК РОССИИ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
по образовательной программе подготовки бакалавров
по направлению 38.03.01 «Экономика»
«Банковское дело»

г. Владивосток
2018

Автор работы Апалькова А.Ю.

_____
(подпись)

«_____» _____ 2018 г.

Руководитель ВКР
д-тор экон. наук, профессор
_____Л.И. Вотинцева
(подпись)

«_____» _____ 2018 г.

Защищена в ГЭК с оценкой _____

Секретарь ГЭК (для ВКР)

_____ _____
(подпись) (Ф.И.О)

«_____» _____ 2018 г.

«Допустить к защите»

Заведующий кафедрой современного банковского дела, канд. экон. наук

_____ А.Н. Слезко
(подпись)

«_____»_____ 2018 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

Базовая кафедра современного банковского дела

З А Д А Н И Е

на выпускную квалификационную работу

Студентке Апальковой Анне Юрьевне *группы* Б1401БДб
(фамилия, имя, отчество)

на тему «Эффективные модели и системы защиты банковской информации: возможности и условия применения на примере ПАО «Сбербанк России»»

Вопросы, подлежащие разработке (исследованию):

Раздел 1 – банковская информация, модели и системы защиты банковской информации в коммерческом банке: цель, задачи, виды банковской информации, правила организации и нормативная база.

Раздел 2 (с приложением фактологического материала, отчетов и т.п. сведений об объекте) – сбор и обработка статистических данных и аналитических оценок по защите банковской информации ДВБ ПАО СБ РФ и его подразделениях в динамике 5лет; ключевые показатели; модели, направленные на минимизацию рисков, связанных с утечкой банковской информации; системы защиты банковской информации, применяемые в ПАО СБ РФ; оценка систем защиты банковской информации, применяемых в ПАО СБ РФ по мнению сотрудников; концепции развития эффективной системы защиты банковской информации .

Основные источники информации и прочее, используемые для разработки темы
учебная литература по теме ВКР; нормативно-законодательные материалы по защите банковской информации в коммерческом банке; стратегии и концепции ПАО СБ РФ по развитию в условиях защиты банковской информации; экономическая и финансовая отчетность банка в динамике 5 лет.

Срок представления работы «_____» _____ 2018 г.

Дата выдачи задания «_____» _____ 2018 г.

Руководитель ВКР д-тор экон. наук, профессор _____ Вотинцева Л.И.
(подпись)

Задание получил _____ Апалькова А.Ю.
(подпись)

Оглавление

Введение

Если рассматривать систему информационной безопасности коммерческого банка с организационной точки зрения, то она представляет собой целостную совокупность элементов, регулярно взаимодействующих между собой посредством методов, мер и средств, которые обеспечивают своевременное предотвращение, выявление, нейтрализацию угроз и защиту интересов коммерческого банка.

Наличие множества компонентов системы позволяет говорить о фундаментальности одних составляющих и второстепенности других. Вместе с тем каждый элемент совокупности имеет важное значение в целях обеспечения ее эффективного функционирования, поскольку нарушение целостности системы способно привести к потере ее устойчивости, а также к полному разрушению. К числу базовых элементов любой экономической системы, в том числе системы безопасности коммерческого банка, принято относить её объект, субъект и механизм функционирования.

Таким образом, главной целью информационной безопасности является обеспечение устойчивого функционирования банка, а также защита информационных ресурсов, принадлежащих банку, его акционерам, инвесторам и клиентам от случайных и направленных противоправных посягательств, разглашения, модификации и уничтожения охраняемых сведений.

Целью выпускной квалификационной работы является обоснование концептуальных подходов к выбору и реализации эффективных моделей современной защиты банковской информации.

Задачи, которые необходимо решить в ходе выполнения работы:

– рассмотреть предпосылки и факторы развития систем защиты банковской информации;

– изучить системы защиты банковской информации;

– исследовать организационные формы и способы обеспечения защиты банковской информации в коммерческом банке;

– выделить базовые требования к системе банковской безопасности в современных условиях;

– проанализировать состояние основных показателей деятельности ПАО Сбербанк в условиях неустойчивой экономической среде;

– изучить объекты, задачи и результаты зашиты банковской информации многофилиального банка на примере ПАО Сбербанк;

– оценить эффективность моделей обеспечения защиты банковской информации в региональных структурах ПАО Сбербанк.

Объектом исследования являются модели и системы защиты банковской информации ПАО «Сбербанк», а предметом исследования – средства, способы и методы защиты банковской информации.

Степень разработанности темы. Теоретические основы научного исследования проблем защиты банковской информации в коммерческих банках представлены в учебных пособиях таких авторов, как Гамза В.А., Корнилов М.Я., Магомедов Б.А. и т.д.

Структура выпускной квалификационной работы определена в соответствии с целью и задачами проекта. Работа состоит из: введения, двух глав, заключения, списка использованных источников и приложения.

1 Объективность и необходимость развития систем защиты банковской информации на современном этапе

1.1 Предпосылки и факторы развития систем защиты банковской информации

Банковская информация – это сведения о субъектах, объектах прав, сделках, иных фактах, событиях, явлениях и процессах, возникающих при осуществлении банковской деятельности.

В самом общем виде банковская информация — это сведения, характеризующие деятельность банка, а также его финансовое состояние, надежность, выполнение требований законодательства и т.п.

Данную информацию можно почерпнуть из устава банки, его лицензий, бухгалтерских балансов, отчетов о прибылях и убытках, и других источников. Кроме того, банковская информация — это сведения о конкретных операциях банка, а также его сотрудниках и клиентах. Такая информация характеризует не только банк, но и тех лиц, с которыми банк вступает в правоотношения [13].

Всю банковскую информацию можно классифицировать по следующим признакам:

– по источнику возникновения: внешняя и внутренняя информация;

– по роли в процессе управления банком: экономическая, социальная, организационно-правовая, технологическая;

– по времени поступления: ежегодная, ежеквартальная, ежемесячная.

По источнику возникновения банковская информация бывает двух видов – внешняя и внутренняя. К внешней информации относятся документы Центрального Банка российской Федерации, Законодательные акты, регулирующие деятельность банков, Постановления Правительства и т.д. К внутренней информации относят: отчетность банка, его внутренние распоряжения и постановления и т.д.

По роли в процессе управления банком выделяют:

– экономическую информацию – это финансовая и экономическая отчетность, характеризующая деятельность банка;

– социальную информацию – это информация и работниках, и клиентах банка;

– организационно-правовую информацию, характеризующая внутреннюю структуру банка, а также органы его управления;

– технологическая информация – это информация о бизнес-процессах внутри банка, его новые технологиях и разработках.

По времени поступления информация бывает ежемесячная, ежеквартальная, полугодовая и ежегодная. Такая классификация чаще всего распространяется на финансовую и экономическую отчетность, которую банки предоставляют в ЦБ РФ.

Прежде чем говорить о защите банковской информации на современном этапе, необходимо определить предпосылки и факторы формирования системы информационной безопасности.

Рассмотрим понятия «факторы» и «предпосылки» обратимся к толковым словарям.

В толковом словаре Ожегова дается следующее определение понятия «предпосылки» - исходные пункты какого-нибудь рассуждения. Предпосылки предварительные условие чего-нибудь.

Понятие «факторы» в толковом словаре Ожегова трактуется как движущая сила, причина какого-нибудь процесса, обусловливающая его или определяющая его характер.

Наиболее значимыми предпосылками, которые оказали влияние на формирование современной защиты банковской информации относятся:

– создание двухуровневой банковской системы, которая требует усиленного контроля и зашиты;

– переход к рыночной экономике;

– налоговая система.

Современная банковская система Российской Федерации сформировалась в результате перестройки государственной финансово-кредитной

системы, сложившейся в период административно-командной экономики. Данная система включала в себя три супербанка-монополиста: Госбанк СССР, Стройбанк СССР и Внешторгбанк СССР, каждый из них выполнял в системе централизованного планового управления экономикой строго определенные функции.

Переход к рыночным реформам потребовал пересмотра сложившейся структуры кредитной системы, функций ее отдельных звеньев и форм организации кредитных отношений. Реформирование государственной банковской системы началось в 1987 г. Оно предусматривало изменение организационной структуры финансово-кредитных учреждений, повышение роли банков в экономической жизни страны [4, с.25].

Первый этап перестройки государственной кредитной системы был реализован в 1987 г., и включал в себя реализацию концепции двухуровневой банковской системы.

Верхний уровень занял Госбанк СССР как центральный банк страны, а нижний - государственные специализированные банки (Промстройбанк СССР, Жилсоцбанк СССР, Агропромбанк СССР, Внешторгбанк СССР, Внешэкономбанк СССР и Сбербанк СССР). На банки второго уровня возлагалось расчетно-кредитное обслуживание соответствующих народнохозяйственных комплексов. Таким образом, произошло углубление отраслевой специализации кредитных учреждений. Госбанк СССР стал осуществлять функции координатора деятельности специализированных банков и проводника единой государственной денежно-кредитной политики.

Второй этап реформирования кредитной системы начался в 1988 г., когда на базе Закона СССР «О кооперации», стали создаваться коммерческие банки на паевой и акционерной основах, в том числе и негосударственные. Фактически была отменена государственная монополия на банковское дело, действовавшая 70 лет, и стали складываться предпосылки для развития реальной конкуренции в финансово-кредитной сфере.

Завершение реформирования банковской системы страны ознаменовалось вступлением в действие новых редакций Законов РФ «О Центральном банке РФ (Банке России)» от 26 апреля 1995 г. и «О банках и банковской деятельности» от 3 февраля 1996 г. В действующем законодательстве закреплены два основных принципа организации банковской системы Российской Федерации:

- двухуровневой структуры банковской системы;
- универсальности банков.

Принцип двухуровневой структуры предусматривает четкое законодательное разделение функций центрального банка и всех остальных банков. Центральный банк Российской Федерации как верхний уровень банковской системы осуществляет функции денежно-кредитного регулирования, банковского надзора и управления расчетной системой страны. Банк России не имеет права проводить банковские операции с юридическими лицами, не являющимися кредитными организациями, и с физическими лицами (кроме военнослужащих и служащих Банка России) [4, с.26].

К факторам, которые повлияли на формирование современных систем защиты банковской информации относят:

- конкуренция;
- количественный и качественный рост банков;
- выход на международный уровень;
- современная политическая обстановка.

В настоящее время деятельность банков регламентируется федеральным законом «О банках и банковской деятельности», в котором введено определение «банковская тайна». В рамках данного закона любая кредитная организация должна обеспечивать сохранность всех данных, касающихся его вкладчиков.

За разглашение данной информации банк несет ответственность, которая включает возмещение ущерба, причиненного клиентам [26, с.159].

Однако, никаких требований к обеспечению информационной безопасности в рамках данного закона не установлено. Это означает что банки самостоятельно

принимают решение по организации информационной защиты основываясь на опыте своих специалистов или сторонних компаний.

При этом, единственной рекомендацией является стандарт ЦБ РФ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». При создании этого ведомственного документа использовались действующие российские и международные стандарты в области информационной безопасности [9, с.230].

Центральный банк Российской Федерации может лишь давать рекомендации другим банкам, но при этом не может настаивать на применении и внедрении тех или иных методов. Кроме того, в стандарте ЦБ РФ нет четких требований к выбору мер по защите банковской информации.

1 января 2007 года был принят федеральный закон «О персональных данных» который установил более жесткие требования к информационной защите банка так как кредитные организации относятся к одним из тех которые работают с персональными данными клиентов. При этом данный закон хоть и является очень важным, но на сегодняшний день не применяется на практике [23, с.135].

Также стоит отметить что большое внимание банки уделяют физической охране как операционных отделений, так и отделений хранения ценностей. Все это снижает риск несанкционированного доступа к коммерческой информации путем физического доступа. Однако офисы банков и технические помещения, в которых размещаются серверы, по степени защиты обычно не отличаются от офисов других компаний. Поэтому для минимизации описанных рисков необходимо использовать систему криптографической защиты.

В Банке на систематической основе проводится мониторинг системы управления и обеспечения КБ как со стороны Управления внутреннего аудита Банка, так и со стороны внешних аудиторов. Результаты проведения мониторинга учитываются при совершенствовании систем управления и обеспечения КБ.

Обеспечение КБ затрагивает каждого сотрудника Банка, использующего его информационные активы, и накладывает на него обязанности и ограничения, направленные на сохранность информационных активов [28, с.14].

Важнейшим элементом деятельности по обеспечению КБ в Банке является повышение осведомленности сотрудников по вопросам ИБ и КБ, предполагающее:

– ведение разъяснительной работы о важности обеспечения ИБ и КБ и информирование персонала об актуальных угрозах КБ и правилах «компьютерной гигиены», в т.ч. путем подготовки мультимедийных и печатных обучающих материалов;

– включение в обучение пользователей независимых тестов реальной реакции на методы социальной инженерии;

– поощрение лиц, сообщающих об уязвимостях в банковских продуктах и сервисах;

– краудсорсинг для вовлечения сотрудников в поиск новых идей по повышению КБ;

– формирование единой культуры КБ у сотрудников Банка [45].

Развитие систем управления и обеспечения КБ Банка и повышение их эффективности достигается путем совершенствования Политики КБ, других внутренних нормативных документов Банка в области КБ, своевременного и должного использования результатов внутренних и внешних аудитов, анализа отслеживаемых событий и лучших мировых практик.

Руководство Банка и коллегиальные органы на регулярной основе рассматривают отчеты о состоянии КБ в подразделениях Банка и о фактах нарушений установленных требований, а также общие и частные вопросы КБ, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы [45].

1.2 Современные модели защиты банковской информации

В соответствии со ст. 20 Федерального закона «Об информации, информатизации и защите информации» целями защиты информации являются в том числе: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Защита данных банковской деятельности содержит в себе осуществление единого комплекса мероприятий — от аудита информационной защищенности и вплоть до формирования концепций защиты различных банковских служб. Эксперты данной сферы готовы сформировать ровно как самостоятельный модуль защищенности, так и полную концентрированную концепцию систему защиты данных [45].

Защита информации банка будет надежно работать только при своевременном определении системой внешних угроз. Во внешней среде системы разделяют следующие виды угроз информации (таблица 1) [44].

Таблица 1 - Виды угроз информации во внешней среде

п/п	Наименование угрозы	Характеристика
1	нарушение физической целостности	уничтожение, разрушение элементов
2	нарушение логической целостности	разрушение логических связей
3	модификация содержания	изменение блоков информации, внешнее навязывание ложной информации
4	нарушение конфиденциальности	разрушение защиты, уменьшение степени защищенности информации
5	нарушение прав собственности на информацию	несанкционированное копирование

Источник: [19]

Планирование систем защиты данных для компании должно содействовать уменьшению вероятных неблагоприятных результатов, связанных с применением информационных технологий, и гарантировать возможность осуществления ключевых целей и задач кредитной организации. Построение моделей при проектировании либо модернизации системы защиты данных в банках является естественным средством решения задач анализа и проектирования с наименьшими расходами и значительной отдачей. В банках используется модель нарушителя информационной безопасности, которая включает в себя:

– описание нарушителей информационной безопасности;

– классификация нарушителей информационной безопасности;

– описание опыта и знаний нарушителей;

– описание доступных ресурсов, необходимых для реализации угрозы;

– описание возможной мотивации действий нарушителя;

– способы реализации угроз информационной безопасности со стороны указанных нарушителей [16].

Для построения модели нарушителя используется информация от службы безопасности, риск-подразделений и службы внутреннего контроля банка о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадии передачи, обработки и хранения, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место случаях хищения информации и т.п.

Помимо этого, оцениваются реальные оперативные технические возможности правонарушителя с целью влияния на концепцию защиты либо на защищаемый объект. Под техническими возможностями понимается перечень разнообразных технических средств, которыми может располагать правонарушитель в ходе совершения операций, нацеленных против системы защиты информации [15].

Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать злоумышленник в процессе совершения действий, направленных против системы защиты информации.

Полезной для оценки последствий действий нарушителя представляется классификация нарушителей безопасности.

Для примера используем в качестве основания цель проникновения в информационную систему организации:

– исследователь (удовлетворение собственного любопытства, развитие профессиональных навыков, анализ разработок и т.д.);

– конкурент (промышленный шпионаж, дискредитация конкурента, получение новых конкурентных преимуществ и т.д.);

– шантажист (получение вознаграждения за не обнародование полученной информации, приобретение нематериальных преимуществ (профессиональный рост, условия контракта, служебные преференции и т.д.));

– террорист (разрушение или применение полученной информации для экстремистских, политических, экономических или экологических целей);

– вредитель (слабомотивированное или немотивированное деструктивное воздействие на информационные ресурсы без ярко выраженной материальной или личностной заинтересованности) [15].

Модель угроз информационной безопасности – описание источников угроз информационной безопасности; методов реализации угроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

Адекватные модели угроз информационной безопасности позволяют выявить существующие угрозы, разработать эффективные контрмеры, повысив тем самым уровень ИБ, и оптимизировать затраты на защиту (сфокусировав её на актуальных угрозах).

У различных информационных систем, а также объектов одной информационной системы может быть разный спектр угроз, определяемый особенностями конкретной информационной системы и её объектов и характером возможных действий источника угрозы [16].

Процедура построения модели угроз информационной безопасности состоит из нескольких последовательных шагов:

– определение источников угроз;

– выявление критических объектов информационной системы;

– определение перечня угроз для каждого критического объекта;

– выявление способов реализации угроз;

– оценка материального ущерба и других последствий возможной реализации угроз [15].

При использовании моделей, как и любого другого инструментария, существуют определенные требования и ограничения, соблюдение которых обеспечивает эффективное решение задач анализа, синтеза и управления в системах информационной безопасности.

– моделями должны пользоваться квалифицированные специалисты-профессионалы в области защиты информации, которые могли бы в каждой конкретной ситуации выбрать наиболее эффективную модель и критически оценить степень адекватности получаемых решений [15];

– модели следует использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании значимых исходных параметров в возможных диапазонах их изменений. В этом плане модели определения значений показателей уязвимости могут служить весьма ценным инструментом при проведении деловых игр по защите информации;

– для оценки адекватности моделей, исходных данных и получаемых решений надо как можно шире привлекать квалифицированных и опытных экспертов.

Модели угроз составляются на основе постоянно меняющихся данных и поэтому должны регулярно пересматриваться и обновляться.

В целях реализации эффективной системы обеспечения информационной безопасности в банке ведется деятельность по идентификации угроз и потенциальных нарушителей информационной безопасности [16].

Оценка рисков производится с учетом модели угроз и нарушителей. Эта оценка используется при принятии организационных и технических решений относительно методов, средств и механизмов защиты информации в системе обеспечения информационной безопасности, а также при осуществлении деятельности по управлению рисками.

Существуют следующие методы обеспечения информационной безопасности банка:

1. **Управление доступом к информационным активам.** Ограничение круга лиц и технологических процессов, имеющих доступ к информационным активам, обеспечивается на уровне прав пользователей и на уровне сети.

Предоставление доступа к информационным системам банка на уровне прав пользователей осуществляется согласно назначенным типовым ролям [38, с.18].

Процедура управления доступом на уровне прав пользователей является сквозной и непрерывной, и длится от момента приема сотрудника на работу до момента его увольнения.

Перед использованием информационных систем пользователь обязан идентифицировать себя с помощью уникального идентификатора пользователя (логина). Идентификатор однозначно идентифицирует пользователя и должен соответствовать принятым правилам именования учетных записей в банке. Использование информационных систем под чужим идентификатором (логином) категорически запрещено. Пользователь несет персональную ответственность за любые действия, совершенные с использованием его учетной записи.

Привилегированный доступ (уровень доступа, предоставляющий полномочия по изменению всех параметров конфигурации, либо параметров безопасности системы, предоставления прав административного, операторского или пользовательского доступа к информационным системам, изменения, удаления всех данных в информационных ресурсах) предоставляется исключительно для выполнения задач, в которых необходим соответствующий уровень доступа. Для каждого информационного ресурса составляется и поддерживается в актуальном состоянии реестр административных учетных записей. Привилегированный доступ к информационным ресурсам должен пересматриваться на регулярной основе [38, с.18].

Защищенный удаленный доступ к информационным ресурсам банка через сеть Интернет предоставляется тем сотрудникам банка, которым он необходим для выполнения своих служебных и функциональных обязанностей. При этом

предоставление удаленного доступа прекращается по истечении служебной необходимости.

Сотрудникам банка предоставляется доступ к ресурсам сети Интернет в рамках выполнения ими служебных обязанностей.

Ключевыми мерами по управлению доступом на сетевом уровне является защита периметра банковской сети и зонирование/сегментирование внутри сети. Хранение информации во внутренней или во внешней сети определяется ее критичностью. Разграничение доступа на уровне сети выполняется средствами межсетевого экранирования (в т.ч. соответствующими встроенными механизмами сетевых маршрутизаторов).

Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

В банке используется набор механизмов и методов, позволяющих обеспечить аутентификацию, авторизацию и разграничение при доступе к информационным активам [38, с.18].

2. Безопасная разработка банковских продуктов. Подразделения, обеспечивающие информационную безопасность совместно с другими заинтересованными подразделениями банка, осуществляют анализ рисков на всех стадиях разработки и внедрения банковских продуктов и услуг, начиная с самых ранних этапов (подготовка концепции), а также принятие адекватных идентифицированным угрозам и рискам мер противодействия.

Банковские услуги предоставляются с оптимальным уровнем безопасности «по умолчанию» (обеспечивающим защищенность от актуальных угроз). Данный уровень определяется для каждой услуги индивидуально в процессе взаимодействия подразделений банка [38, с.19].

При создании банковских продуктов необходимо предусматривать возможность перехода в «красную тактику» – заранее согласованные владельцем бизнес-продукта и дополнительные меры по управлению риском (временное ограничение функциональности продукта, изменение уровня предоставляемого

сервиса т.п.) как ответ на повышение уровня операционного риска свыше установленного порога.

Безопасность программного кода банковского ПО обеспечивается на всех стадиях жизненного цикла. Это достигается путем:

– использования специализированных систем и процедур контроля на наличие ошибок и недокументированных возможностей;

– контроля за внедрением ПО для критичных АБС и внесением в него изменений, контроля целостности кода в процессе эксплуатации [38, с.19].

3. Управление инцидентами кибербезопасности. Управление инцидентами кибербезопасности является одним из важнейших мероприятий в деятельности банка по обеспечению информационной защиты и осуществляется в целях минимизации ущерба, вызванного реализованной угрозой, максимально быстрого устранения последствий кибератак, консолидации статистики по инцидентам кибербезопасности, выявления причин возникновения инцидентов и принятия упреждающих мер по исключению подобных ситуаций в будущем [38, с.20].

Каждый сотрудник банка, допущенный к работе с корпоративными информационными системами, обязан знать признаки нарушения информационной безопасности и кибербезопасности. Для этого организуется необходимое обучение или инструктаж пользователей.

О возникновении инцидента кибербезопасности (в т.ч. подозрении на него) каждый сотрудник банка обязан незамедлительно сообщить Администратору информационной безопасности и руководителю своего подразделения.

4. Обеспечение непрерывности бизнеса. Непрерывность бизнеса заключается в выполнении банком в условиях чрезвычайных ситуаций (экономических и политических кризисов, природных и техногенных катастроф, террористических угроз и т.д.) на минимально необходимом уровне функций, без которых деятельность банка невозможна.

Мероприятия по обеспечению непрерывности включают в себя создание процедур резервирования и восстановления функций банка, в том числе для

чрезвычайных ситуаций невысокой вероятности возникновения. Необходимость резервирования и восстановления функций определяется оценкой ущерба от их прерывания [38, с.19].

Непрерывность бизнеса подразумевает также обеспечение непрерывности и надежности средств защиты. Надежность средств защиты не должна быть меньше надежности защищаемой системы; данные показатели определяются лицами, ответственными за обеспечение функционирования средств защиты и защищаемой системы [38, с.20].

1.3 Организационные формы и способы обеспечения защиты банковской информации в коммерческом банке

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности банка определяются реальными потребностями банка и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью.

Организация и функционирование системы безопасности должны соответствовать следующим принципам [26]:

1. Повышение качества и ценности бизнес-продуктов. Кибербезопасность создает ценность для бизнеса не только путем предотвращения потерь, но и повышением качества продуктов. В цифровом бизнесе ни один продукт не может быть качественным, если он небезопасен.

2. Системность. При обеспечении кибербезопасности (далее – КБ) Банка учитываются все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, значимые с точки зрения КБ. При создании

системы обеспечения КБ учитываются все слабые и наиболее уязвимые места, а также характер и возможные направления кибератак.

3. Непрерывность. Обеспечение КБ Банка представляет собой непрерывно совершенствуемый процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИТ и информационных систем [38, с.7].

4. Обоснованность и простота применения средств защиты. Меры по обеспечению КБ реализуются на современном уровне развития технологий, и должны быть достаточными для защиты от актуальных угроз КБ, понятными и простыми в применении. Использование средств защиты не может быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе пользователей.

5. Обязательность контроля. Необходимо обеспечивать обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения КБ. Контроль над деятельностью любого пользователя, ИТ-системы, средства защиты осуществляется на основе применения средств оперативного мониторинга и регистрации событий и охватывает как несанкционированные, так и санкционированные действия [38, с.8].

6. Обнаружение и реагирование. Банком обеспечивается обнаружение и реагирование на угрозы с учетом перехода от «data-центричной» к «человеко-центричной» модели безопасности: мониторинг инцидентов и событий должен опираться на анализ поведения пользователей и учетных записей (модель UEBA – User and Entity Behavior Analysis).

7. Соответствие нормативным требованиям. Обеспечение КБ Банка осуществляется в соответствии с положениями и требованиями действующих нормативных правовых актов Российской Федерации в области ИБ и КБ, применимых норм международного права, а также ВНД Банка. Обеспечение КБ также основывается на применимых отечественных и международных стандартах и нормативно-методических документах органов государственной власти.

8. Инновационность и развитие компетенций. В Банке на постоянной основе проводится исследовательская работа по поиску, изучению и реализации в продуктах и услугах оптимальных решений в области КБ, которая включает [38, с.8]:

– использование в качестве методологии построения технологии КБ требований международных и национальных стандартов;

– изучение передового опыта (в том числе международного), технологий и решений в части обеспечения КБ;

– адаптацию и внедрение лучших технологий обеспечения КБ в продукты и услуги Банка;

– использование технологий Big Data для решения задач КБ;

– поиск новых высокотехнологичных и надежных решений защиты с использованием технологии краудсорсинга;

– организацию и проведение открытых конкурсов на создание инновационных решений в области КБ;

– взаимодействие с вузами по развитию компетенций в области КБ.

9. Совершенствование культуры кибербезопасности. Проводится реализация мер по повышению культуры КБ сотрудников и клиентов, включая обучение безопасному использованию цифровых сервисов, в том числе пониманию рисков, связанных с использованием цифровых сервисов и размещением в них информации. При этом создаются условия, при которых любой реализовавшийся риск будет иметь последствия для лица, явившегося причиной этого (принцип «неотвратимости наказания») [38, с.9].

10. Централизация управления. Банк проводит единую политику КБ, в том числе по вопросам обработки персональных данных, использования криптографических средств, лицензирования деятельности. При необходимости ЦА актуализирует требования по обеспечению КБ с учетом специфических условий, имеющихся в организационно-подчиненных подразделениях.

11. Идентификация информационных активов. У каждого информационного актива определяется его владелец, категория обрабатываемой в

нем информации, уровень критичности и индивидуальные требования по обеспечению КБ. Средствами АС ведется реестр информационных активов; его ведение входит в полномочия и область ответственности блока «Технологии», см. п.5.11 настоящего документа [38, с.9].

12. Классификация информации по уровням критичности. Информация, обрабатываемая в Банке, классифицируется по степени влияния фактов ее разглашения на деятельность Банка и его положение на рынке. Допускается одновременное использование нескольких систем классификации информации.

13. Минимизация привилегий. Доступ к информационным активам сотруднику Банка предоставляется в том минимальном объеме, который необходим ему для выполнения служебных обязанностей.

14. Персональная ответственность и разделение обязанностей. Ответственность за обеспечение КБ Банка возлагается на каждого сотрудника в пределах его полномочий. Распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае нарушения круг нарушителей был четко определен. В Банке разделены функции подразделений и обязанности сотрудников Банка, осуществляющих администрирование коммуникационного оборудования, ОС, СУБД, прикладных информационных систем, средств защиты, мониторинга состояния КБ и контроля (аудита) выполнения требований по обеспечению КБ [38, с.9].

15. Принцип «двух персон». Выполнение критичных банковских операций проводится двумя сотрудниками. При обслуживании клиентов – физических лиц лучшей практикой считается возложение подтверждения операции в качестве «второй персоны» на клиента в рамках клиентской сессии. Исходя из уровня идентифицированных рисков и при согласовании с Департаментом безопасности (ДБ), возможность единоличного совершения операции одним сотрудником допускается для ограниченного набора операций в рамках установленных лимитов и иных ограничений (по сумме, количеству, времени, должности, территориальному признаку, другим показателям). Автоматизированные банковские системы (АБС) обеспечивают автоматический контроль соответствия

параметров операций установленным лимитам и ограничениям. Принцип «двух персон» также применяется при изменении критичных параметров ИТ-инфраструктуры, АС и средств защиты информации;

16. Сочетание риск-ориентированного подхода и подхода на основе требований. К функционированию и совершенствованию системы обеспечения КБ применяются риск-ориентированный подход и подход на основе требований (обязательных для выполнения правил и условий) КБ. Меры по обеспечению безопасности информационных активов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков КБ. КБ не ограничивается запретительными мерами, но отвечает на актуальные запросы бизнеса, разъясняет возникающие риски и предлагает решения по их минимизации [38, с.9].

Основными участниками защиты банковской информации в коммерческом банке являются:

– Президент, Председатель Правления Банка;
– Правление Банка;
– Управляющий комитет Банка по рискам кибербезопасности;
– Самостоятельные структурные подразделения Банка;
– Территориальные банки;
– Головные отделения Банк;
– Руководители самостоятельных структурных подразделений;
– Администраторы информационной безопасности.

Президент, Председатель Правления Банка осуществляет общее руководство системой управления и обеспечения КБ в Банке [38, с.26].

Правление Банка:

– утверждает Стратегию КБ и Политику КБ Банка;
– рассматривает отчеты о состоянии КБ в Банке;
– определяет политику взаимоотношений с государственными органами в вопросах обеспечения КБ [38, с.26].

Управляющий комитет Банка по рискам кибербезопасности является постоянно действующим рабочим органом Банка, принимающим решения по управлению рисками КБ. Целью деятельности УК является принятие решений, обеспечивающих баланс между развитием бизнеса и достаточным уровнем КБ, а также формирование эффективной системы управления рисками КБ. УК подотчетен Комитету Банка по рискам Группы и Правлению Банка [38, с.27].

Самостоятельные структурные подразделения Банка:

– обеспечивают регистрацию инцидентов, потенциально являющихся инцидентами КБ, силами Администраторов ИБ подразделения, а также осуществляют передачу информации в ДБ;

– устанавливают в пределах своей компетенции порядок доступа и правила работы с информационными активами в киберпространстве, владельцами которых они являются;

– участвуют совместно с ДБ в оценке рисков реализации угроз информационным активам Банка в киберпространстве;

– учитывают требования и риски КБ при разработке новых, модификации существующих продуктов и услуг;

– разрабатывают нормативные и распорядительные документы с учетом требований КБ;

– обеспечивают при управлении компаниями Группы Банка (в рамках кураторства и координации) выполнение этими компаниями политик, стандартов и требований КБ, а также согласованных планов в области развития КБ [38, с.27].

Территориальные банки (ТБ) выполняют функции, предусмотренные ВНД и ОРД Банка, в том числе:

– разработка распорядительных документов на уровне ТБ по вопросам обеспечения КБ;

– доведение до сотрудников ВНД по вопросам КБ;

– участие в проведении служебных расследований случаев мошенничества персонала Банка, совершаемого с использованием, АС Банка, а также инцидентов КБ в АС;

– взаимодействие с Управлением внутреннего аудита по результатам проверок выполнения требований по обеспечению КБ;

– взаимодействие с территориальными органами государственной власти по вопросам КБ, в пределах своей компетенции;

– организация обучения сотрудников ТБ по вопросам КБ [38, с.27].

Головные отделения Банка (ГОСБ) выполняют функции, предусмотренные ВНД и ОРД Банка, в том числе:

– разработка распорядительных документов на уровне ГОСБ по вопросам обеспечения КБ;

– участие в проведении расследований случаев несанкционированного использования АС;

– взаимодействие с территориальными органами государственной власти по вопросам КБ, в пределах своей компетенции;

– организация обучения сотрудников ГОСБ по вопросам КБ [15].

Руководители самостоятельных структурных подразделений:

– несут персональную ответственность за организацию и состояние системы обеспечения КБ в подчиненном подразделении, включая обеспечение безопасности обрабатываемых персональных данных;

– осуществляют руководство работой по обеспечению КБ в подразделении, обеспечивают выполнение сотрудниками подразделения требований КБ;

– назначают Администраторов ИБ подразделения и руководят их работой;

– принимают решения о предоставлении прав доступа сотрудникам подчиненного подразделения к информации, согласовывают эти решения в установленном порядке;

– принимают решения о предоставлении прав доступа к информации, владельцем которой является подразделение, сотрудникам других подразделений по обращению руководителей этих подразделений, согласовывают эти решения в установленном порядке;

– определяют категории информации, владельцем которой является подразделение;

– назначают ответственного за действия сотрудников сторонней организации во внутренней корпоративной сети Банка (при заключении по инициативе подразделения договора со сторонней организацией);

– несут ответственность за действия сотрудников сторонней организации во внутренней корпоративной сети Банка (при отсутствии назначенного ответственного);

– взаимодействуют с Подразделениями КБ по вопросам организации системы обеспечения КБ в подразделении [38, с.28].

Администратор ИБ – сотрудник, назначаемый в каждом структурном подразделении руководителем. На Администратора ИБ возлагаются следующие обязанности:

– проведение инструктажа сотрудников подразделения по вопросам КБ и ИБ;

– контроль проведения антивирусных мероприятий и соблюдения других требований по обеспечению КБ и ИБ;

– обеспечение и контроль доступа пользователей к информационным ресурсам Банка;

– взаимодействие с Подразделениями КБ по инцидентам КБ и ИБ [16].

Кроме этого, стоит отметить базовые требования по обеспечению информационной безопасности банка.

Для обеспечения кибербезопасности в Банке применяется масштабный комплекс технических средств, механизмов и технологий защиты информации, в состав которого входят специализированные устройства и ПО, средства мониторинга, встроенные механизмы защиты ОС, СУБД, информационных систем (приложений), телекоммуникационного оборудования и других устройств.

Управление техническими средствами и механизмами защиты информации осуществляют (в зоне своей ответственности) ДБ и подразделения блока «Технологии».

Технические решения в области КБ создаются в рамках проектной деятельности и проходят все стадии разработки, включая оценку с последующим учетом в финансово-экономическом обосновании проекта, разработку и реализацию проектных решений, тестирование, опытную эксплуатацию, приемку и передачу в промышленную эксплуатацию.

На этапе создания любой информационной системы или банковского продукта к нему предъявляются требования со стороны ДБ; данные требования должны быть реализованы при помощи технических средств и механизмов и/или организационных мер. Переход по этапам жизненного цикла всех информационных систем Банка (в том числе ввод в опытную, промышленную эксплуатацию, вывод из эксплуатации) происходит по согласованию с ДБ.

Для отдельных сервисов и систем ДБ разрабатываются частные политики КБ и модели угроз [38, с.15].

Банковская внутренняя и внешняя сети должны быть разделены шлюзами прикладного уровня; хранение информации во внутренней или во внешней сети определяется ее критичностью, что является необходимой компенсационной мерой по отношению к потенциалу нарушителя [38, с.15].

Защите от вредоносного ПО (компьютерных вирусов, «червей», троянских программ) принадлежит ключевая роль в обеспечении заданного уровня обеспечения КБ в Банке. Эта область обеспечения безопасности затрагивает каждого сотрудника, допущенного к работе с корпоративными информационными системами.

Защита от вредоносного ПО реализуется как на уровне прикладных информационных потоков и централизованных сервисов, так и на уровне отдельных компьютеров. В Банке применяются меры по борьбе с вредоносным ПО, создаваемым, в том числе, для реализации целенаправленных атак (Advanced Persistent Threat, APT) на Группу Банка [16].

Для обеспечения конфиденциальности критичной информации при передаче по каналам связи и хранении за пределами защищенного периметра, а также в иных требующих этого случаях, применяется шифрование.

Средства криптографической защиты информации, используемые для решения задач обеспечения КБ в Банке, применяются в соответствии с действующей нормативно-правовой базой в этой области.

Для обеспечения аутентичности и/или целостности критичной информации применяется электронная подпись (ЭП). В зависимости от ситуации могут применяться простая ЭП (PIN-код, одноразовый пароль), неквалифицированная либо квалифицированная ЭП. Могут применяться и другие механизмы, установленные внешними и внутренними требованиями.

Для управления ключами ЭП в Банке развернут удостоверяющий центр [38, с.5].

Использование облачных технологий и личных мобильных устройств рассматривается Банком как объективная реальность и возможность повышения эффективности основной деятельности. Вместе с тем, учитывая повышенные риски использования этих технологий, необходимо принятие дополнительных мер обеспечения КБ.

Хранение (в том числе кратковременное) банковской информации на ресурсах, не принадлежащих Банку, в обязательном порядке согласуется с ДБ.

Банк устанавливает ограничения и требования по безопасному использованию личных мобильных устройств (принцип «BYOD – Bring Your Own Device») [21].

2 Оценка возможностей и условия применения систем защиты банковской информации в ПАО Сбербанк

2.1 Состояние основных показателей деятельности банка в условиях неустойчивой экономической среде

Проанализируем состояние основных показателей деятельности ПАО Сбербанк в условия неустойчивой экономической среде с целью оценки эффективности применения систем защиты банковской информации.

Проведем анализ ликвидности и надежности ПАО Сбербанк по его основным показателям за последние 5 лет.

Таблица 2 – Показатели ликвидности и надежность ПАО Сбербанк 2013-2017 гг. (млрд. руб.)

Показатель	**01.01.2014**	**01.01.2015**	**изменение за 12 мес.**	**01.01.2016**	**изменение за 12 мес.**	**01.01.2017**	**изменение за 12 мес.**	**01.01.2018**	**изменение за 12 мес.**	**изменение за 5 лет**
средства в кассе	639,97	1 138,24	**498,27**	625,86	**-512,38**	500,2	**-125,66**	547,19	**46,99**	**-92,78**
средства на счетах в Банке России	296,67	227,15	**-69,52**	468,32	**241,17**	812,5	**344,18**	589,25	**-223,25**	**292,58**
корсчета НОСТРО в банках (чистых)	112,46	380,74	**268,28**	411,75	**31,01**	362,71	**-49,04**	312,13	**-50,58**	**199,67**
межбанковские кредиты, размещенные на срок до 30 дней	223,79	353,74	**129,95**	799,32	**445,58**	674,98	**-124,34**	637,94	**-37,04**	**414,15**
высоколиквидные ценные бумаги РФ	212,76	527,27	**314,51**	1037,99	**510,72**	1049,99	**12**	1118,7	**68,71**	**905,94**
высоколиквидные ценные бумаги банков и государств	35,41	28,93	**-6,48**	216,83	**187,90**	17,6	**-199,23**	40,2	**22,6**	**4,79**
Высоколиквидные активы с учетом дисконтов и корректировок (на основе Указания №3269-У от 31.05.2014)	**1516,17**	**2651,16**	**1 134,99**	**3527,55**	**876,39**	**3415,39**	**-112,16**	**3239,4**	**-175,99**	**1723,23**

Источник: [14]

На основе данных, представленных в таблице 2 можно сделать следующие выводы:

1. Объем средств в кассе в период с 2013 по 2017 гг. имел нестабильную динамику, это мы можем наблюдать на рисунке 1 (приложение А). Так на по состоянию на 01.01.2014 данный показатель находился на отметке 639,97 млрд. руб. за 2014 год произошло увеличение на 498,27 млрд. руб. и по состоянию на

01.01.2015 г. достиг отметки 1 138,24 млрд. руб. Несмотря на значительный рост, объемы денежных средств в кассе банка за 2015 год показали отрицательную динамику, которая наблюдалась вплоть до 2017 года.

2. ПАО Сбербанк начиная с 2013 года снизил средства на счетах в Банке России, данную динамику мы можем наблюдать на рисунке 2 (приложение Б). Однако в 2015 году вновь увеличил данные резервы более чем в два раза, в 2016 году ПАО Сбербанк также увеличил свои резервы в Банке России более чем в два раза. Однако в 2017 году, данный показатель вновь пошел на спад.

3. В целом, можно сказать, что все показатели, отвечающие за ликвидность ПАО Сбербанк, имели нестабильную динамику, которую можно наблюдать на рисунках 3,4,5,6 и 7 (приложение В, Г, Д, Е и Ж), то есть на протяжении пяти лет то снижались, то увеличивались.

Далее рассмотри показатели, характеризующие структуру и динамику баланса.

Таблица 3 – Показатели структуры и динамики баланса ПАО Сбербанк 2013-2017 гг. (млрд. руб.)

Показатель	**01.01.2014**	**01.01.2015**	**изменение за 12 мес.**	**01.01.2016**	**изменение за 12 мес.**	**01.01.2017**	**изменение за 12 мес.**	**01.01.2018**	**изменение за 12 мес.**	**изменение за 5 лет**
Межбанковские кредиты	597,68	864,68	**267,00**	1 136,95	**272,27**	2 023,27	**886,32**	1 846,61	**-176,66**	**1 248,93**
Кредиты юр.лицам	7 872,19	10 802,95	**2 930,76**	11 904,88	**1 101,93**	10 361,57	**-1 543,31**	10 955,32	**593,75**	**3 083,13**
Кредиты физ.лицам	3 332,84	4 069,34	**736,50**	4 129,16	**59,82**	4 333,35	**204,19**	4 924,52	**591,17**	**1 591,68**
Вложения в ценные бумаги	2 267,24	2 036,51	**-230,73**	2 924,12	**887,61**	2 802,27	**-121,85**	3 308,33	**506,06**	**1 041,09**
Прочие доходные ссуды	632,17	792,98	**160,81**	803,14	**10,16**	738,88	**-64,26**	765,61	**26,73**	**133,44**
Доходные активы	**14 817,57**	**19 599,73**	**4 782,16**	**21 412,63**	**1 812,90**	**20 460,78**	**-951,85**	**21 910,48**	**1 449,70**	**7 092,91**

Источник: [14]

Проанализировав данные таблицы 3 можно сделать следующие выводы:

1. Объем выданных межбанковских кредитов в период с 2013 по 2017 гг. вырос более чем в три раза, данное изменение можно наблюдать на рисунке 8 (приложение З). Однако, динамика данного показателя в течении пяти лет была нестабильной, так в период с 2013 по 2016 гг. данный показатель демонстрировал

положительную динамику, но по состоянию на 01.0.12018 уменьшился на 223,34 млн. руб.

2. Объемы выданных кредитов юридическим лицам, также в течении пяти лет выросли более чем в 1,5 раза, данные изменения представлены на рисунке 9 (приложение И). Однако, в 2016 году он пошел на спад, но по состоянию на 01.01.2018 г. вновь показал положительную динамику.

3. Что касается кредитования физических лиц, то за 2013-2017 гг., данный показатель имел только положительную динамику и за пять лет увеличился более чем в 1,6 раз, рисунок 10 (приложение К).

4. Вложения в ценные бумаги и в прочие доходные активы за 2013-20177 гг. также имели нестабильную динамику, за 2013-2015 гг. ПАО Сбербанк наращивал данные вложения, а в 2016 году показали небольшой отрицательный рост, однако, по состоянию на 01.01.2018 г. данные вложения вновь приняли положительную динамику (приложение Л, М).

5. В целом, можно сказать, что вложения в доходные активы в период с 2013 по 2017 гг. увеличились в 1,5 раза, несмотря на незначительные снижения в 2016 году (приложение Н).

Далее рассмотри показатели, характеризующие прибыльность ПАО Сбербанк, а также изменение данные показателей в течении 5 лет.

1. За 2013 год прибыльность источников собственных средств (рассчитываемая по балансовым данным) уменьшилась за год с 20.88% до 20.13%. При этом рентабельность капитала ROE увеличилась за год с 33.08% до 42.88%.

Чистая процентная маржа уменьшилась за год с 5.33% до 5.17%. Доходность ссудных операций увеличилась за год с 11.26% до 11.47%. Стоимость привлеченных средств увеличилась за год с 3.94% до 4.28%. Стоимость средств населения (физ. лиц) увеличилась за год с 3.97% до 4.34%.

2. За 2014 год прибыльность источников собственных средств (рассчитываемая по балансовым данным) уменьшилась за год с 20.13% до 15.71%. При этом рентабельность капитала ROE уменьшилась за год с 42.88% до 18.43%.

Чистая процентная маржа уменьшилась за год с 5.17% до 4.97%. Доходность ссудных операций незначительно изменилась за год с 11.47% до 11.44%. Стоимость привлеченных средств увеличилась за год с 4.28% до 4.58%. Стоимость средств населения (физ. лиц) уменьшилась за год с 4.34% до 3.91%.

3. За 2015 год прибыльность источников собственных средств (рассчитываемая по балансовым данным) уменьшилась за год с 15.71% до 10.04%. При этом рентабельность капитала ROE за год с 18.43% до 11.32%.

Чистая процентная маржа уменьшилась за год с 4.97% до 3.83%. Доходность ссудных операций увеличилась за год с 11.44% до 11.70%. Стоимость привлеченных средств увеличилась за год с 4.58% до 6.23%. Стоимость средств населения (физ. лиц) увеличилась за год с 3.91% до 5.65%.

4. За 2016 год прибыльность источников собственных средств увеличилась за год с 10.04% до 18.19%. При этом рентабельность капитала ROE увеличилась за год с 11.32% до 23.51%.

Чистая процентная маржа увеличилась за год с 3.83% до 5.15%. Доходность ссудных операций незначительно изменилась за год с 11.70% до 11.78%. Стоимость привлеченных средств уменьшилась за год с 6.23% до 4.63%. Стоимость средств населения (физ. лиц) уменьшилась за год с 5.65% до 4.96%.

5. За 2017 года прибыльность источников собственных средств (рассчитываемая по балансовым данным) увеличилась за год с 18.19% до 19.94%. При этом рентабельность капитала ROE увеличилась за год с 23.51% до 24.82%.

Чистая процентная маржа увеличилась за год с 5.15% до 5.61%. Доходность ссудных операций уменьшилась за год с 11.78% до 11.35%. Стоимость привлеченных средств уменьшилась за год с 4.63% до 3.96%. Стоимость средств населения (физ. лиц) уменьшилась за год с 4.96% до 4.04%.

Таким образом, можно сделать вывод, что на сегодняшний день Сбербанк успешно осуществляет свою банковскую деятельность, поскольку за последние пять лет обороты по его операциям увеличились более чем в 1,5 раз, это говорит о том, несмотря на воздействие внешних негативных факторов, таких как

экономический кризис, санкции и т.д. ПАО Сбербанк обеспечивает достойную защиту банковской информации и банковской тайны.

2.2 Объекты, задачи и результаты защиты банковской информации многофилиального банка на примере ПАО Сбербанк

В ноябре 2017 года в ПАО Сбербанк был утвержден «Протокол Кибербезопасности ПАО Сбербанк», в котором отражены цели и задачи, основные объекты, способы и методы защиты банковской информации.

Так, система обеспечения и управления информационной безопасности ПАО Сбербанк ориентирована на достижение следующих целей:

– обеспечение цифровой устойчивости бизнеса банка и компаний, входящих в группу Банка;

– предоставление безопасного обслуживания клиентам;

– обеспечение уровня риска КБ, необходимого для обеспечения устойчивого развития банка [38, с.5].

Для достижения поставленных целей банком решаются следующие задачи:

– организация проактивной защиты: обеспечение опережающего реагирования на существующие и потенциальные угрозы безопасности банка и клиентов за счет поиска и использования инновационных подходов, методов управления, технологий обеспечения информационной безопасности и всестороннего оперативного мониторинга состояния кибербезопасности (далее – КБ) [38, с.5].;

– внедрение КБ в культуру повседневной деятельности сотрудников и клиентов банка с использованием всех возможных информационных каналов, современных методов и средств обучения;

– создание системы управления и обеспечения КБ на основе риск-ориентированного подхода: принятие управленческих решений в области КБ по результатам анализа, оценки и обработки рисков КБ;

– обеспечение безопасности периметра киберпространства банка, включая современные методы и средства идентификации и аутентификации клиентов, и сотрудников [38, с.6].;

– обеспечение безопасной разработки банковских продуктов;

– организация противодействия различным видам мошенничества, обеспечение взаимодействия подразделений центрального аппарата банка и Группы Банка при обработке случаев хищений;

– реализация в группе банка единых политик и стандартов по управлению и архитектуре систем КБ;

– формирование новых компетенций КБ, включая взаимодействие с вузами и приобретение лучших специалистов на рынке труда;

– организация эффективного взаимодействия с государственными институтами, средствами массовой информации и профессиональными сообществами для обмена информацией об угрозах КБ и мерах противодействия.

Также, в данном протоколе прописаны объекты защиты банковской информации в ПАО Сбербанк, а именно [39, с.45].:

– информационные ресурсы, которые содержат коммерческую или банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы банка, независимо от формы и вида ее представления;

– информационные ресурсы, которые содержат конфиденциальную информацию, включая персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы банка, независимо от формы и вида ее представления;

– сотрудники банка, которые являются разработчиками и пользователями информационных систем Сбербанка;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и

телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы [38, с.45].

Также в протоколе об «Информационной политике Сбербанка» дается определение целей и задач по обеспечению информационной защиты Сбербанка.

Целью деятельности по обеспечению информационной безопасности Сбербанка является снижение угроз информационной безопасности до приемлемого для банка уровня.

Основные задачи деятельности по обеспечению информационной безопасности банка:

– выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

– предотвращение инцидентов информационной безопасности;

– исключение либо минимизация выявленных угроз.

Если мы говорим об обеспечении информационной безопасности одного из самых крупных банков России, то необходимо оценить насколько эффективно осуществляется данный процесс.

Необходимо понимать насколько эффективно Сбербанк работает по направлению защиты банковской информации, а также обеспечению кибербезопасности.

21 октября 20085 года Наблюдательный Совет Сбербанка одобрил стратегию развития Сбербанка до 2014 года, в которой основными направлениями деятельности в области защиты банковской информации были следующие пункты:

– обеспечение информационной безопасности Банка;

– противодействие преступным посягательствам на устройства самообслуживания Банка;

– противодействие мошенничеству с использованием поддельных документов;

– обеспечение физической охраны объектов Банка [14, с.123].

За 6 лет осуществления своей деятельности в рамках данной стратегии Сбербанк добился значительных результатов, а также реализовал практически все поставленные перед ним задачи.

Несмотря на значительный рост преступных посягательств на устройства самообслуживания (665 случаев, рост на 24%), ущерб Банка от хищений денежной наличности из устройств самообслуживания за шесть лет сократился на 33%.

Относительно 20008 года Банку удалось сократить количество хищений устройств самообслуживания с 98 до 16 случаев. Охраняющие организации, прибывшие по сигналам «тревога» от устройств, задержали 376 злоумышленников.

С помощью технических средств охраны предотвращено 500 попыток хищения денежных средств из УС на 3,1 млрд руб. Благодаря работе системы фрод-мониторинга предотвращенные убытки по скимингу за 2014 год составили порядка 4,7 млрд руб. При этом переход на чиповые карты, внедрение антискимингового оборудования и активная борьба с установщиками нештатного оборудования обеспечили устойчивую тенденцию снижения случаев компрометации и уровня убытков Банка [14, с. 124].

За шесть лет выявлено 3423 случая установки скимингового оборудования на УС. Изъят 141 комплект устройств. На месте преступления при активном содействии подразделений экономической безопасности сотрудниками правоохранительных органов задержано 77 человек.

В 2014 году Сбербанк утвердил Концепцию по оснащению своих устройств самообслуживания системой видеоконтроля. Реализация Концепции существенно повысит уровень технической защищенности устройств.

В области экономической безопасности Банк работал над усовершенствованием механизма взаимодействия служб безопасности, андеррайтинга и Блока Риски во всех сегментах кредитования. Сумма предотвращенного потенциального ущерба в результате отказа в выдаче кредитов корпоративным клиентам в связи с выявлением подразделениями экономической безопасности негативной информации, а также фактов предоставления клиентами фиктивных документов составляет более 136,6 млрд руб. При проверке кредитных

заявок по технологии «Кредитная фабрика» было выявлено 929 заявок, содержащих фиктивные сведения и документы, подтверждающие доход и трудовую занятость заемщика. При попытках получения кредитов по фиктивным документам правоохранительными органами задержано 43 человека. Сумма предотвращенного ущерба составила более 1,2 млрд руб [14, с. 52].

Сотрудники подразделений безопасности Банка выполняют новый функционал, связанный с обеспечением экономической безопасности дочерних банков дальнего и ближнего зарубежья, выявлением угроз интересам Группы Сбербанка. За шесть лет выявлена негативная и существенная информация по участникам 190 сделок дочерних банков с зарубежными контрагентами.

Подразделениями информационной безопасности внедрены технологии выявления мошеннических операций, которые в 2014 году выявили и пресекли 71 попытку хищения средств юридических и свыше 87 тыс. попыток хищения средств физических лиц. Предотвращен ущерб на сумму 2,9 млрд руб.

В 2014 году правоохранительными органами при взаимодействии с подразделениями информационной безопасности Сбербанка прекращена деятельность трех киберпреступных групп, осуществляющих массовые атаки на клиентов Банка. Задержано и привлечено к ответственности 7 человек. Приоритетные объекты Банка оснащаются современными высокотехнологичными интегрированными системами безопасности ведущих мировых производителей. Среди таких объектов – Кассово-инкассаторский центр и Корпоративный университет Банка.

После реализации Стратегии развития Сбербанка до 2014 года, была утверждена Стратегии информационной безопасности ОАО «Сбербанк России» 2014-2018гг.

Для достижения целей в развитии информационной безопасности Сбербанк было разработано 4 основных направлений [14, с.45].

1. Реализация новой архитектуры приложений. Осуществление эволюционной трансформации существующей автоматизированной банковской системы (АБС) в России в централизованную, надежную платформу с высоким

уровнем автоматизации и модульными принципами построения, а также постепенный переход к единой платформе для фронт-офисных систем.

2. Модернизация технологической платформы. Консолидация существующих территориально распределенных центров обработки данных, завершение создания единой глобальной сети.

3. Создание новой операционной модели в ИТ. Повышение уровеня согласованности и качество взаимодействия между ИТ-службами и их внутренними клиентами. Создание новой операционной модели в ИТ, в том числе пересмотрев наиболее критические процессы и компетенции в рамках подготовительной фазы до начала масштабных работ по архитектуре приложений.

4. Кибербезопасность. Усиление защиты персональных данных и укреплением кибербезопасности. С увеличением количества удаленных транзакций, которые совершают наши клиенты, вопросы безопасности данных становятся критически важными [14, с. 123].

9 июня 2018 года состоялось Общее собрание акционеров, на котором Председатель Правления ПАО Сбербанк Герман Греф представил акционерам годовой отчет в рамках Стратегии развития Сбербанка 2014-2018 гг.

Стоит отметить, что за три года реализации данной Стратегии Сбербанк добился значительных результатов в развитии систем защиты банковской информации.

– 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».

Экономическая безопасность является безусловным приоритетом для Сбербанка. В 2014-2017 г. было выявлено и предотвращено 529 случаев использования похищенных (утерянных) или поддельных паспортов, выявлено 22 попытки мошенничества с применением поддельных платежных документов и предотвращено хищение денежных средств со вкладов клиентов Сбербанка по 71 поддельной доверенности на общую сумму 600 млн руб, [14, с.145].

Всего подразделениями экономической безопасности за три года было направлено 1055 заявлений в правоохранительные органы по факту попыток причинения ущерба Сбербанку или его клиентам, при этом было возбуждено 526 уголовных дел.

В 2017 году было выявлено 4041 поддельных и умышленно поврежденных (составных) купюр, при этом идентифицировано 80 массовых вбросов. В подразделениях Сбербанка и Корпоративно-инвестиционного центра было выявлено 949 случаев предъявления клиентами поддельных банкнот Банка России. Также из оборота было изъято 1577 поддельных банкнот различного номинала.

В 2017 году применение искусственного интеллекта и аналитических измерений для определения мошеннических операций, при которых клиент добровольно передает информацию мошенникам, позволило хеджировать около 97% такого риска со стороны клиента. За 2017 год было пресечено более 300 тыс. попыток хищения средств физических и юридических лиц, предотвращен ущерб на сумму более 40 млрд руб, [14, с.45].

Сбербанк уделяет особое внимание кибербезопасности. Банк научился успешно противодействовать киберпреступности с помощью интеллектуальной системы защиты клиентов. Так, проект Сбербанка «Фрод-мониторинг для удаленных каналов обслуживания физических лиц» стал бронзовым призером меж - дународного конкурса IPMA International Project Excellence Award 2017. В рамках масштабного проекта, который длился 15 месяцев, в Сбербанке была внедрена уникальная система фрод-мониторинга, созданная на основе искусственного

интеллекта. Система в автоматическом режиме защищает клиентов от некорректных действий, вызванных недостаточным знанием, правил кибербезопасности. Еженедельно с помощью этой системы выявляется несколько тысяч подозрительных операций. В 2018 году продолжится развитие системы противодействия кибермошенничеству с целью обеспечить 100% защиту всех каналов обслуживания клиентов Сбербанка [14].

Обеспечение защиты персональных данных в Сбербанке осуществляется в рамках единой комплексной системы организационно-технических и правовых мер по защите конфиденциальной информации (коммерческая, банковская тайна, персональные данные.

Однако, на сегодняшний день существует немало угроз информационной безопасности коммерческого банка, в связи с этим Сбербанк принял новую Стратегию развития до 2020 года, в которой основными направлениями в области развития систем информационной безопасности выделены следующие аспекты.

– обеспечение 100% защиты всех каналов обслуживания клиентов Сбербанка.

– разработка и внедрение единого сервиса аутентификации и собственного сервиса цифровой подписи, а также создание единого Cybersecurity Fusion Centre, в котором будут внедрены технологии искусственного интеллекта, машинного обучения и больших данных для обеспечения централизованного управления кибербезопасностью Группы Сбербанк.

– развитие международных отношений, которые позволят предложить новые форматы программы Академии кибербезопасности, а также будет развивать и выводить на рынок новые услуги в сфере кибербезопасности.

2.3 Оценка эффективности моделей обеспечения защиты банковской информации в региональных структурах ПАО Сбербанк

В протоколе об «Информационной политике Сбербанка» от 13.09.2016 г., утвержденном Наблюдательным советом ПАО «Сбербанк» говорится о том, что банк действует в режиме информационной открытости по отношению ко всем

целевым аудиториям. Кроме того, доступ к публичной информации, за исключением информации, которая составляет коммерческую или банковскую тайну, предоставляется банком на безвозмездной основе и не требует выполнения специальных процедур (получения паролей, регистрации или иных технических ограничений) для ознакомления с ней.

Стоит отметить, что грамотная организация защиты банковской информации позволяет вовремя отследить и выявить нарушения по использованию и передачи коммерческой и банковской тайны, а также простимулировать сотрудников банка соблюдать правила.

Организационная защита коммерческой и банковской тайны выполняет функции по:

- организации охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз.

Рассмотрим подробно элементы защиты банковской информации, которые применяются в ПАО «Сбербанк»:

- во всех отделениях, а также на территории, прилагаемой к отделениям ПАО «Сбербанк» установлены камеры видеонаблюдения, а также шлагбаумы для исключения тайного проникновения посторонних лиц на территорию банка;
- каждый сотрудник перед трудоустройством на работу в ПАО «Сбербанк» проходит инструктаж «О хранении и использовании конфиденциальной информации и персональных данных клиентов», а также подписывает лист ознакомления, в соответствии с которым, он принимает на себя ответственность за разглашение информации, которая составляет коммерческую или банковскую тайну;
- доступ к информационным ресурсам ПАО «Сбербанк» предоставляется в соответствии с занимаемой должностью сотрудника, а также его разрядом (грейдом);

– регулярное обучение и тестирование сотрудников на предмет обращения с персональными данными клиентов, а также информацией, которая составляет коммерческую или банковскую тайну;

– обмен банковской информацией происходит только во внутренней сети Сбербанка, компьютеры, на которых хранится и используется конфиденциальная информация не имеют доступа в Интернет;

– в ПАО «Сбербанк» есть служба Сбербанк Сервис (далее – СБС), которая отвечает за информационную безопасность Сбербанка.

Таким образом, можно сказать, что с организационной точки зрения в ПАО «Сбербанк» созданы все условия, которые позволяют защищать банковскую информацию, а также пресекать любые попытки ее распространения.

Однако, стоит подробнее рассмотреть, как средства защиты применяются для сотрудников Сбербанка, а также используются сотрудниками Сбербанка каждый день.

1. Все сотрудники Сбербанка имеют пропуски в формате пластиковых магнитных карточек или наручного браслета, на этом пропуске имеется информация: ФИО сотрудника, а также структурное подразделения банка, в котором работает владелец данного пропуска. Принцип действия таких карточек очень прост. Данная система позволяет отследить перемещение сотрудника по банку, а именно позволяет отследить, когда сотрудник пришел на работу, когда он с нее ушел, а также посмотреть, когда и куда он заходил. Таким образом, все перемещения сотрудников фиксируются, тем самым позволяют контролировать и предотвращать утечку банковской информации.

2. Каждый сотрудник Сбербанка имеет ЭЦП (электронная цифровая подпись). При приеме на работу, сотруднику присваивается учетная запись, в которую он может войти только при помощи ЭЦП, который представляет собой ключик (как от домофона). На данной ЭЦП хранится информация о должности и разряде сотрудника, которая ограничивает или наоборот увеличивает диапазон информации, к которой он имеет доступ. Кроме того, данный ключ, служит еще и электронной подписью сотрудника, таким образом, все документы и запросы он

может подписывать своей ЭЦП. ЭЦП является именной и не подлежит передачи третьему лицу.

3. Все компьютеры во внутренней сети банка не подключены к интернету, а также просматриваются службой безопасности, таким образом, техник в любой время может подключится к компьютеру сотрудника и заблокировать его действия, если произойдет попытка передачи третьим лицам информации, которая составляет банковскую или коммерческую тайну.

4. Каждые три месяца все сотрудники банка проходят обязательное обучение по хранению и передачи конфиденциальной информации. Это позволяет банку контролировать, а также напоминает своим подчиненным, что бывает за передачу банковской информации третьим лицам.

5. Вся техника, которая принадлежит ПАО «Сбербанк», а именно планшеты, ноутбуки, компьютеры, находятся под наблюдением служб безопасности, таким образом, сотрудникам запрещается входить в данные компьютерные приборы под своей личной учетной записью.

Однако, Сбербанк заботится не только о защите банковской информации на территории, но и за ее пределами, а именно система охраны и контроля за всеми сотрудниками, а также предметами, которые приносятся на территорию банка и выносятся с нее. Рассмотри некоторые их них:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (доступу) злоумышленников на объекты защиты (территорию, в здание и помещения) и материальными носителями. Например, заборы, стальные двери, кодовые замки, сейфы и т. д.;
- средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и др. технических средств управления;
- средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализации, информирования и идентификации);

– средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.);

– технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т.п.

– средства противопожарной охраны;

– средства защиты помещений от визуальных способов технической разведки.

В связи с этим в целях повышения экономической безопасности ПАО «Сбербанк» уделяет большое внимание подбору и изучения кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи. При этом в обязательном порядке проводить значительную разъяснительно-воспитательную работу, систематические инструктажи и учения по правилам и мерам безопасности, регулярные, но неожиданные тестирования различных категорий сотрудников по постоянно обновляемым программам.

В контрактах ПАО «Сбербанк» четко очерчивает персональные функциональные обязанности всех категорий сотрудников Банка и на основе существующего российского законодательства во внутренних приказах и распоряжениях определяет их ответственность за любые виды нарушений, связанных с разглашением или утечкой информации, составляющей коммерческую тайну.

Кроме того, Банк все шире вводит в своих служебных документах гриф «конфиденциально» и распространяет различного рода надбавки к окладам для соответствующих категорий своего персонала.

Среди сотрудников ПАО Сбербанк Приморского отделения 8635, являющихся руководителями различных подразделений был проведен опрос о защите банковской информации в ПАО Сбербанк.

В рамках данного опроса была разработана анкета участника (приложение О). Респондентам, в количестве 20 человек, было задано шесть вопросов об

организации системы защиты банковской информации, применяемой в ПАО Сбербанк. Рассмотрим, результаты опроса.

Для начала участникам опроса был задан вопрос: «Работаете ли Вы с банковской информацией?», на который все 20 человек ответили положительно (приложение П).

Далее респондентам был задан вопрос, в котором участники описали банковскую информацию, с которой они работают каждый день (приложение Р).

Большинство респондентов указало, что каждый день в своей работе они используют отчеты о деятельности подразделения, руководителями которых они являются.

Поскольку опрос проводился среди руководителей различных подразделений, то на втором месте по частоте использования банковской информации стоят персональные данные сотрудников, а именно размер оплаты труда, графики отпусков, больничные листы и т.д.

Кроме того, в своей работе руководитель структурных подразделений также и используют персональные данные клиентов, однако, это не те персональные данные, которые мы привыкли видеть с вами. Чаще всего это данные, касающиеся деятельности клиентов, а именно отчеты и результаты деятельности компании, паспортные данные сотрудников предприятия и т.д.

Также в своей работе руководители подразделений используют стандарты работы, штатное расписание и нормативные документы ПАО Сбербанк.

Участникам был задан вопрос относительно их роли в обеспечении защиты банковской информации, а именно являются ли они АИБами (администраторами информационной безопасности). В соответствии с приложением С, 86% опрошенных на данный вопрос ответило отрицательно.

Стоит отметить, что в ПАО Сбербанк руководители подразделений не являются администраторами информационной безопасности, так как данная роль ограничивает спектр возможностей руководителя, например он не может подтверждать заявки на предоставление доступов в банковские программы, поэтому чаще всего администраторами информационной безопасности являются

заместители руководителя, аналитики, координаторы и т.д., а руководитель является согласующим звеном.

На вопрос «Какими средствами защиты банковской информации пользуетесь Вы каждый день?» большинство респондентов отметили ЭЦП (электронная цифровая подпись).

Данный инструмент защиты банковской информации все сотрудники банка применяют каждый день, без данного ключа ни одни сотрудник банка не сможет зайти в компьютер, а также в банковские программы.

Второй по частоте ответ среди респондентов был – пароль к личной учетной записи, а также электронные пропуска.

Стоит отметить, что при использовании как личной учетной записи, так и электронных пропусков сотрудники, обеспечивающие информационную и техническую безопасность банка, могут в режиме онлайн наблюдать за действиями всех сотрудников, а именно о его передвижениях по офису, а также использование банковских программ во внутренней сети банка.

Далее респондентам был задан вопрос: «Как вы считаете в ПАО Сбербанк эффективная система защиты банковской информации?», на который лишь 87% опрошенных дали положительный ответ.

Таким образом, в ходе данного опроса были выявлены проблемы, а также были предложены решения по улучшению систем защиты банковской информации ПАО Сбербанк.

Стоит отметить, что на сегодняшний день система защиты ПАО Сбербанк является одной из самых эффективных и надежных, данные выводы были сделаны на основании результатов деятельности защиты банковской информации многофилиального банка на примере ПАО Сбербанк.

2.4 Концепции развития эффективной информационной защиты в ПАО Сбербанк в условиях осложнения глобальной экономической ситуации

На основе данных о результатах деятельности ПАО Сбербанк в области защиты банковской информации и опроса сотрудников Сбербанка Приморского

ГОСБ 8635, являющихся руководителями подразделений были выявлены концепции развития эффективной информационной защиты ПАО Сбербанк в условиях осложнения глобальной экономической ситуации.

2. В связи с повышенным контролем и применением многоуровневой защиты информации при ее передачи многие банковские программы замедляют свою работу, что приводит к замедлению работы самого человека, а иногда даже целого отдела. Например, при передачи персональных данных клиентов через электронную почту во внутренней сети банка необходимо использовать систему шифрования, таким образом, передача информации заминает порядка 30 минут – 2 часов. В связи с этим, сотрудниками Сбербанка, а также его руководства было принято решение об отменен шифрования сообщений при обмене персональных данных во внутренней сети, что значительно укорило процесс работы. Однако, при передаче во внешние источники, обходимо также шифровать сообщения.

3. При применении сотрудникам электронных пропусков, на которых записана основная информация по сотруднику ПАО сбербанк нередко происходит сбой в системе, в результате которого сотрудники не могут попасть на свои рабочие места, так как данная система просто блокирует данные электронные пропуска, а именно стирается вся информация с чипов, расположенных в электронных пропусках, и по пропуску войти нельзя. В связи с этим, необходимо так настроить пропускную систему, чтобы даже при малейших ее сбоях сотрудники ПАО Сбербанк могли попасть на свои рабочие места, например ввести идентификацию сотрудников по отпечаткам пальцев. Такой метод применяется во многих европейских странах.

4. В связи с тем, что вся техника контролируется службами безопасности банка, а также программистами, то в любое время может начать обновляться система или же устанавливаться новое ПО, что заметно осложняет работу, так как сотрудники могут попросту не сохранить определенные документы что приводит к уничтожение результатов работы нескольких дней. В связи с этим необходимо заранее предупреждать сотрудников о вмешательстве служб безопасности и ИТ-служб в работу банка.

Данные концепции были разработаны в соответствии с ответами руководителей подразделений ПАО Сбербанк Приморского ГОСБ 8635 при проведении опроса об информационной защите ПАО Сбербанк.

Кроме того, нами были выведены концепции развития эффективной информационной защиты согласно годовым отчетам акционерам ПАО Сбербанк, а также Стратегии развития ПАО Сбербанк до 2020 года.

1. Разработка и внедрение единого сервиса аутентификации и собственного сервиса цифровой подписи, а также создание единого Cybersecurity Fusion Centre, в котором будут внедрены технологии искусственного интеллекта, машинного обучения и больших данных для обеспечения централизованного управления кибербезопасностью Группы Сбербанк. Таким образом, развитие и внедрение искусственного интеллекта в работу Группы Сбербанка позволит эффективнее управлять информационной защитой, поскольку данный процесс будет автоматизирован и контроль за сохранением банковской информации будет вестись в режиме онлайн 24 часа в сутки.

2. Перевод клиентов, продуктов и данных на новую платформу, которая будет реализована на инновационной облачной инфраструктуре, использующей технологии быстрых вычислений «в памяти», и будет обеспечивать высокий уровень надежности и доступности.

3. Обеспечение защиты данных клиентов и инвестирование в инструменты мониторинга и защиты всех цифровых каналов, создание центра мониторинга всех операций, обучение сотрудников, клиентов и партнеров современным способам предотвращения киберпреступлений. Таким образом, не только сотрудники ПАО Сбербанк будут обладать информацией как предотвратить хищение конфиденциальной информации, но и клиенты банка будут в полной мере обучены всем тонкостям предотвращения случаев киберпреступности, что значительно снизит убытки и ущерб банка.

Заключение

Таким образом, можно сказать, что цель выпускной квалификационной работы достигнута и поставленные задачи решены

Выявлено, что базовой основой организации эффективной защиты банковской информации служат современные модели, формы и способы обеспечения защиты банковской информации.

Опираясь на такую научную основу, нами оценено состояние систем защиты банковской информации.

Критериями оценки эффективности защиты банковской информации послужили:

– Ключевые показатели деятельности ПАО Сбербанк в период с 2013 по 2017 гг.;

– Соблюдение принципов защиты банковской информации;

– Оценка действующих моделей защиты банковской информации, применяемых в ПАО Сбербанк.

В результате прослеживается относительно устойчивая повышающаяся тенденция ключевых показателей деятельности ПАО Сбербанк, что недвусмысленно отражается на содержании и результатах защиты банковской информации.

Сегодня, основными задачами защиты банковской информации являются 6 основным направлений, прописанных в Стратегии развития ПАО Сбербанк до 2020 года. Однако, Сбербанк максимально сосредоточен на выполнении следующих задач по защите банковской информации:

– обеспечение 100% защиты всех каналов обслуживания клиентов Сбербанка.

– разработка и внедрение единого сервиса аутентификации и собственного сервиса цифровой подписи, а также создание единого Cybersecurity Fusion Centre, в котором будут внедрены технологии искусственного интеллекта,

машинного обучения и больших данных для обеспечения централизованного управления кибербезопасностью Группы Сбербанк.

развитие международных отношений, которые позволят предложить новые форматы программы Академии кибербезопасности, а также будет развивать и выводить на рынок новые услуги в сфере кибербезопасности.

Кроме того, гипотетически предполагаем, что эффективность в области защиты банковской информации не достигнута, этот результат подтвердил опрос, в котором сотрудники Сбербанка выявили следующие проблемы в области защиты банковской информации:

– многоуровневая защита информации, которая замедляет работу;

– сбой в программах и устройствах, обеспечивающих защиты банковской информации;

– неконтролируемое обновление систем и программ, которое приводит к остановке и замедлении работы банка.

В результате, нами была разработана концепция развития эффективной системы защиты банковской информации ПАО Сбербанк, включающая:

– Отказ от многоуровневого согласования и проверки документов, передающихся во внутренней сети банка;

– Переход от физических средств охраны ПАО Сбербанк к инновационным, включающих считывание роговицы глаза, отпечаток пальца и т.д.;

– Обучение сотрудников и клиентов ПАО Сбербанк приемам, позволяющие отразить попытки кибератак.

Список использованных источников

1. О банках и банковской деятельности: федер. закон от 02.12.1990 №395 -1: принят Гос. Думой 02.12.1990 г. [ред. от 29.12.2015]. – Электрон. дан. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=196350
2. О Центральном банке Российской Федерации: федер. закон от 10.07.2002 №86 -ФЗ: принят Гос. Думой 27.06.2002 г. [ред. от 30.12.2015]. – Электрон. дан. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=183030
3. Алавердов А.Р. Организация и управление безопасностью в финансово-кредитных организациях: Учеб. пособие. М., 2014.
4. Аленин В. В., Груздева Е. В. Экономическая безопасность банковской системы и мониторинг кредитных организаций в регионе (теоретические и прикладные аспекты): учебное пособие для вузов / под ред. профессора А. Г. Кайгородова. Иваново: ИГХТУ, 2011. С. 136.
5. Афанасьев М. новый метод оценки бизнес - идеи инвестиционного проекта. // М. Афанасьев / Инвестиции в России, - 2012, -№ 12-с. 29-36.
6. Банковское дело [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://knigi-uchebniki.ru/bankovskoe-delo/
7. Басовский Л.Е., Басовская Е.А. Комплексный экономический анализ хозяйственной деятельности: учеб. Пособие - М.: ИН-ФРА-М, 2011.-366 с.
8. Банк России: борьба с утечками информации необходима [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/The_Bank_of_Russia_combat_leaks_information_necessary
9. Борзенко И.Е. Банковская деятельность. - М.: Экспо, 2005, 415
10. Выявленные случаи неправомерного использования инсайдерской информации и манипулирования рынком [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://www.cbr.ru/finmarket/inside/inside_detect/

11. Гадомская Т. Е. Экономическая безопасность национальной банковской системы. Иваново: Изд-во «Талка», 2015.

12. Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка: учебно-практическое пособие. М.: Издатель Шумилова И. И., 2010.

13. Гапоненко В.Ф., Беспалько А.Л., Власков А.С. Экономическая безопасность предприятий. Подходы и принципы. М.: Изд-во «Ось-89», 2007. С. 21.

14. Годовые отчеты [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://www.sberbank.com/ru/investor-relations/reports-and-publications/annual-reports

15. Защита банковской информации [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://rus.safensoft.com/security.phtml?c=884

16. Защита банковской информации [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://www.osp.ru/cio/2007/06/4253252/

17. ИНСАЙДЕРСКАЯ ИНФОРМАЦИЯ [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://sberbank-pb.ru/insajderskaa-informacia

18. Инсайд и манипулирование [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://www.sberbank.com/ru/compliance/im

19. Информационная безопасность банков [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://tvoi.biz/biznes/informatsionnaya-bezopasnost/informatsionnaya-bezopasnost-bankov.html

20. ИНФОРМАЦИОННАЯ ПОЛИТИКА [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://www.sberbank.com/portalserver/content/atom/contentRepository/content/Информационная%20политика%20(рус).pdf?id=bfd7e3d2-a660-4909-9156-85201377e18f

21. Колесников, В.И. Банковское дело: учебник / Под ред. В.И. Колесникова, Л. П. Кроливецкой, - М., Финансы и статистика, 2014. – 410с.

22. Корнилов М.Я. Экономическая безопасность России: основы теории и методологии исследования: Учебное пособие - М.: Изд. РАГС, 2010 - 154с.

23. Королев М.И. Экономическая безопасность фирмы, практика, выбор стратегии / М.И. Королев - М.: Экономика, 2011 - 284с.

24. Концепция долгосрочного социально-экономического развития РФ до 2020 года - М.: Правительство РФ от, 17 ноября 2008 г. № 1662 - Р.

25. Концепция комплексной защиты информационных банковских систем и сетей [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://eos.ibi.spb.ru/umk/5_14/5/5_R0_T6.html

26. Крылов Э.И. Принципы управления инвестиционной и инновационной деятельностью // Э.И. Крылов, - СПб. 2013. -24 с.

27. Костерина, Т.М. Банковское дело: учебник/ Под редакцией Т.М. Костерина–М.: Экономистъ, 2013. -240с.

28. Лаврушин, О.И. Банки и банковские операции: учебник / Под ред. О.И. Лаврушина.- М.:КНОРУС, 2012- 272 с.

29. Лаврушин, О.И. Банковское дело: учебник / Под ред. О.И. Лаврушина.- М.: КНОРУС, 2014 – 766 с.

30. Лаврушин, О.И. Деньги, кредит, банки: учебник/ Под ред. О.И. Лаврушина – М: КНОРУС, 2015 – 490 с.

31. Магомедов Б. А. Организационно-экономический механизм безопасного развития банковской системы: диссертация на соискание ученой степени кандидата экономических наук. Махачкала, 2013. С. 29.

32. Мак-Мак В. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности. М.: Мир безопасности, 2009. С. 78.

33. Мельников Ю. Н., Теренин А. А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак // Банковские технологии. 2013.

34. Морунов В.В. Экономическая безопасность как экономическая категория // Экономические науки. 2011. № 10. С. 53.

35. Необходимость и особенности банковского менеджмента [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://knowledge.allbest.ru/bank/2c0b65625a3ad78a4c53a88421206d37_0.html

36. Петров В.А., Пискарев С.А., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. - М., 2008.

37. ПОЛОЖЕНИЕ о раскрытии информации Открытого акционерного общества «Сбербанк России» [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://www.sberbank.com/common/img/uploaded/files/pdf/normative_docs/emitter_information_regulations_22022013.pdf

38. Протокол Кибербезопасности ПАО Сбербанк, 2017 г. – с. 32

39. Рейтинговая система показателей [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://koet.syktsu.ru/vestnik/2012/2012-3/7/7.htm

40. Рождественская Т.Э. Банковское право для экономистов: учебник и практикум для бакалавриата и магистратуры / Т.Э. Рождественская, А.Г. Гузнов, А.В. Шам-раев. М.: Изд-во Юрайт, 2015. С. 21.

41. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2012.

42. Саркисянц, Б. А. Российская банковская система: специфика развития/ Саркисянец Б.А.// Бухгалтерия и банки. – М., 2013. - С. 36-44.

43. Сбербанк подтвердил утечку личных данных клиентов [Электрон. ресурс]. – Электрон. дан. – Режим доступа: http://naar.ru/news/sberbank-podtverdil-utechku-lichnykh-dannykh-klientov

44. Способы защиты банковской информации [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://oaookb.ru/articles/sposoby-zashchity-bankovskoy-informacii

45. Способы защиты информации [Электрон. ресурс]. – Электрон. дан. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/

46. Тавасиев, А. М. Банковское дело: учебник/ А.М. Тавасиев - М.: Юрайт, 2013 - 656 с.

47. Тавасиев, А. М., Организация деятельности коммерческих банков. Теория и практика: учебник/А.М. Тавасиев, В.Д. Мехряков, О.И. Ларина - М.: Юрайт, 2014 - 736 с.

48. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 2017 г.

49. Управление деятельностью коммерческого банка (банковский менеджмент) / Под. ред. О. И. Лаврушина. — М.: ЮРИСТЪ, 2015. — 688 с.

50. Ярочкин В. И. Безопасность банковских систем. - М. : Ось-89, 2014. - 416 с.

Приложение

Приложение А

Средства в кассе ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок А – Средства в кассе ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Б

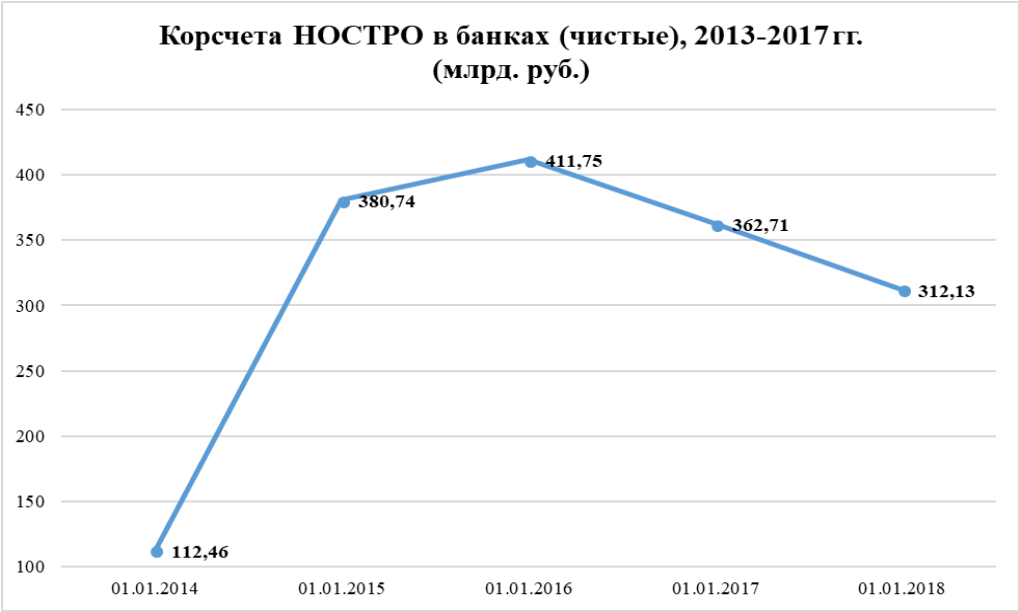
Средства на счетах в Банке России, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок Б – Средства на счетах в Банке России ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение В

Корсчета НОСТРО в банках (чистые) ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)



Источник: [14]

Рисунок В – Корсчета НОСТРО в банках (чистые) ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Г

Межбанковские кредиты, размещенные на срок до 30 дней ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок Г – Межбанковские кредиты, размещенные на срок до 30 дней ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Д

Высоколиквидные ценные бумаги РФ ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник:

Рисунок Д – Высоколиквидные ценные бумаги РФ ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Е

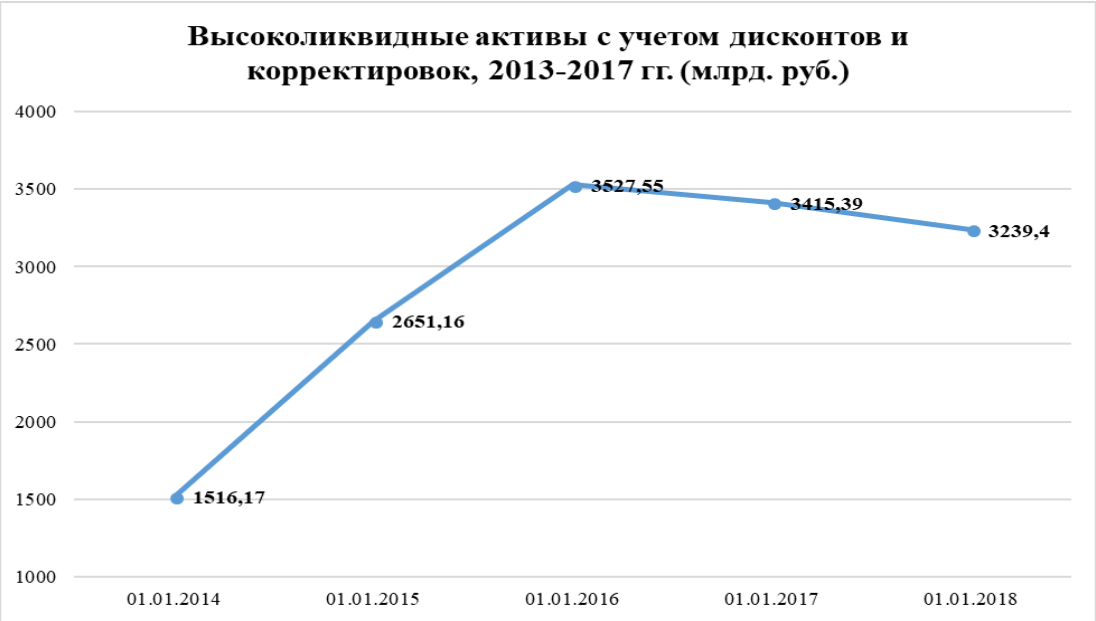
Высоколиквидные ценные бумаги банков и государств ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок Е – Высоколиквидные ценные бумаги банков и государств ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Ж

Высоколиквидные активы с учетом дисконтов и корректировок ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)



Источник: [14]

Рисунок Ж – Высоколиквидные активы с учетом дисконтов и корректировок ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение З

Межбанковские кредиты ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок З – Межбанковские кредиты ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение И

Кредиты юридическим лицам ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок И – Кредиты юридическим лицам ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение К

Кредиты физическим лицам ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок К – Кредиты физическим лицам ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Л

Вложения в ценные бумаги ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок Л – Вложения в ценные бумаги ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение М

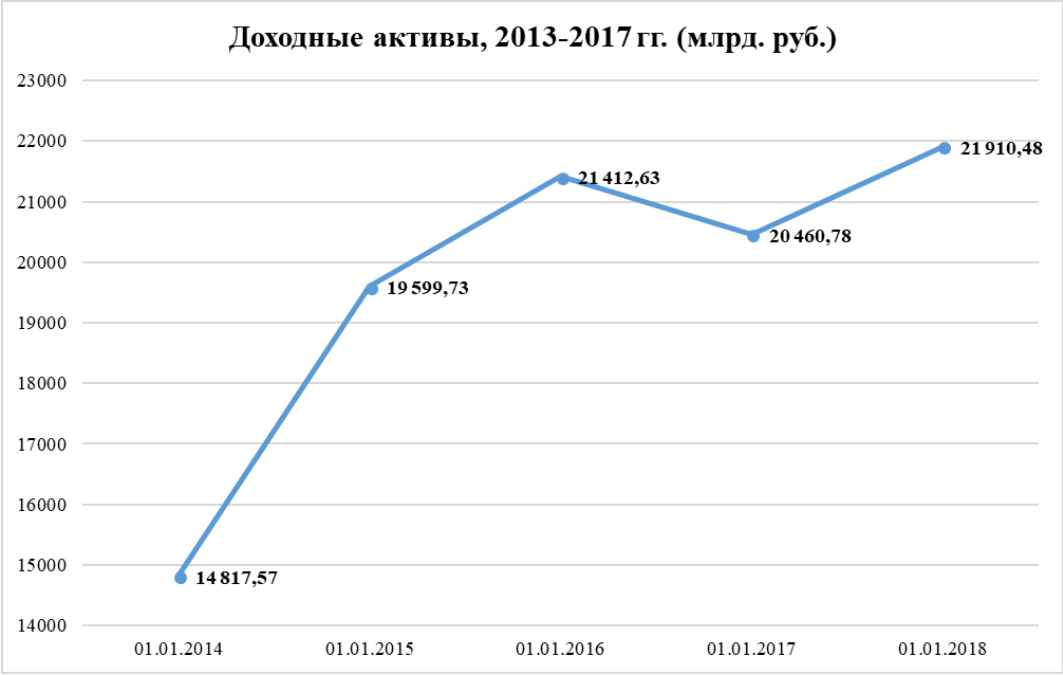
Прочие доходные ссуды ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Источник: [14]

Рисунок М – Прочие доходные ссуды ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение Н

Доходные активы ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)



Источник: [14]

Рисунок Н – Доходные активы ПАО Сбербанк, 2013-2017 гг. (млрд. руб.)

Приложение О

Анкета участника

1. ***Работаете ли Вы с банковской информацией?***
   - ДА
   - НЕТ
2. ***С какой именно банковской информацией Вы работаете? (перечислите информацию, ресурсы и данные, которые Вы используете в своей работе)***
3. ***Являетесь ли Вы АИБом (администратором информационной безопасности)?***
   - ДА
   - НЕТ
4. ***Какими средствами защиты банковской информации пользуетесь Вы каждый день?***
5. ***Как Вы считаете в ПАО Сбербанк эффективная система защиты банковской информации?***

Приложение П

Работаете ли Вы с банковской информацией?

Рисунок П – «Работаете ли Вы с банковской информацией?»

Приложение Р

С какой банковской информацией Вы работаете?

Рисунок Р – «С какой банковской информацией Вы работаете?»

Приложение С

Являетесь ли Вы АИБом?

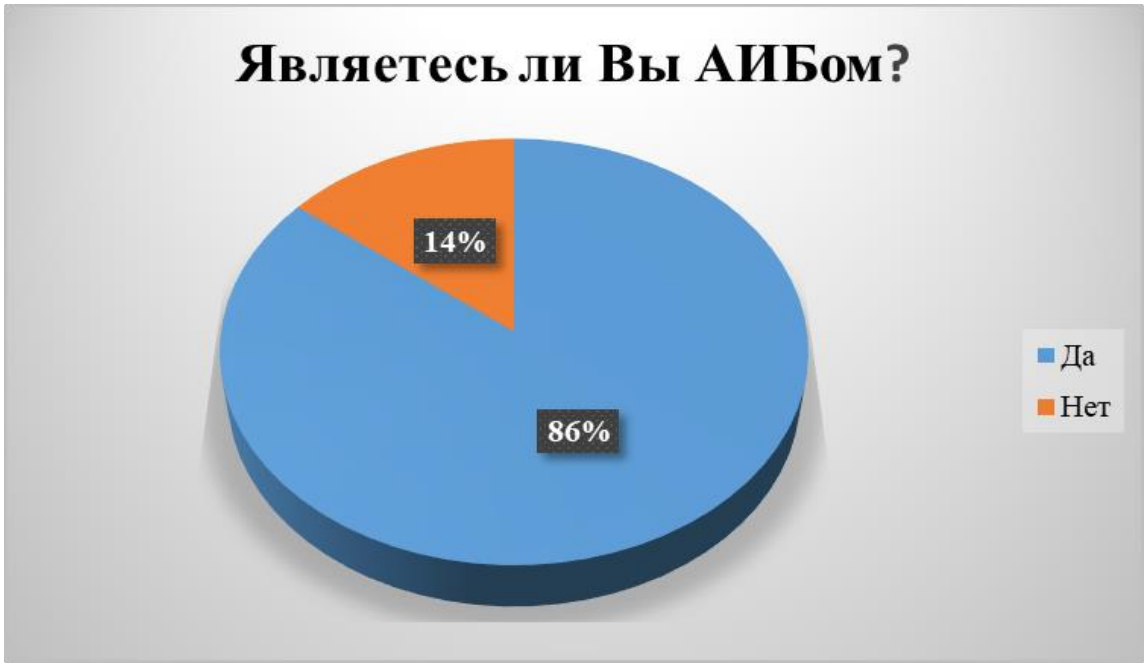


Рисунок С – «Являетесь ли Вы АИБом?»

Приложение Т

Какими средствами защиты банковской информации пользуетесь Вы каждый день?

Рисунок Т – «Какими средствами защиты банковской информации пользуетесь Вы каждый день?»

Приложение У

Как Вы считаете в ПАО Сбербанк эффективная система защиты банковской информации?

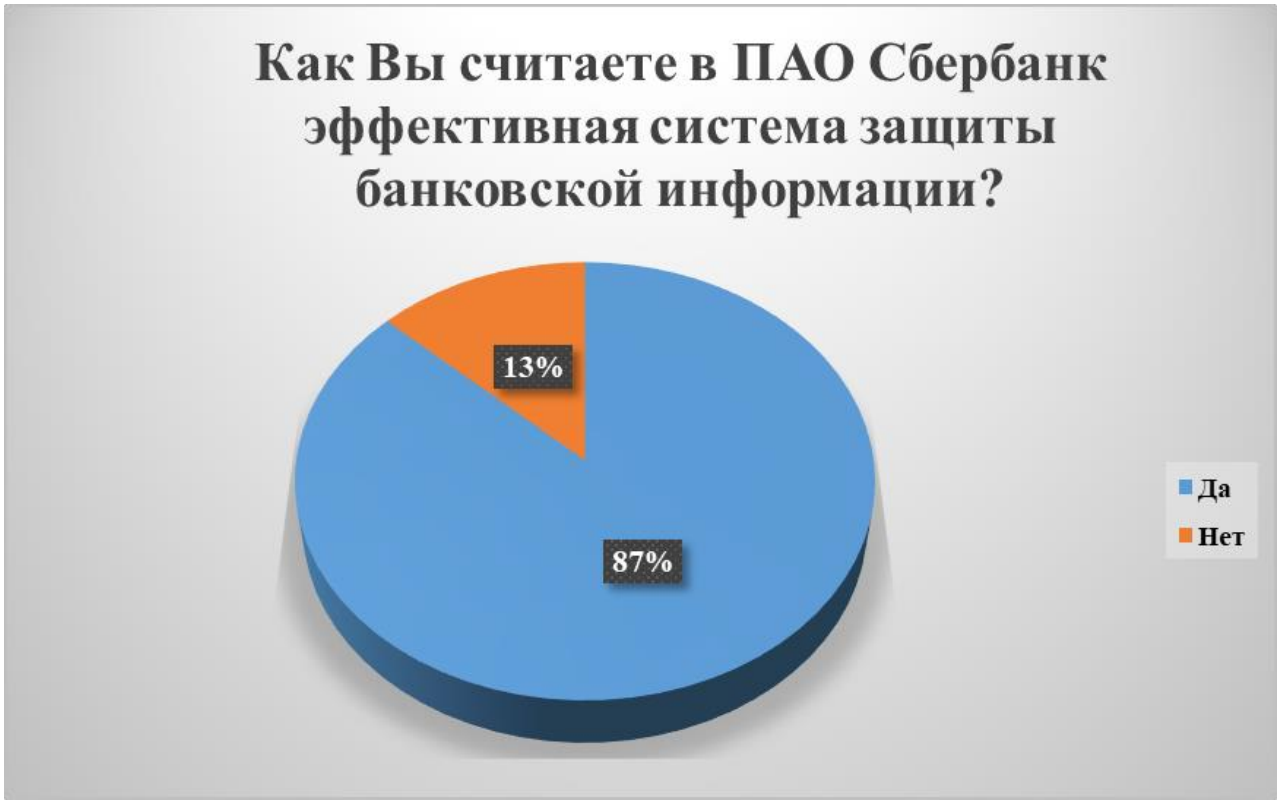


Рисунок У – «Как Вы считаете в ПАО Сбербанк эффективная система защиты банковской информации?»

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Дальневосточный федеральный университет»

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

Кафедра экономической теории

ОТЗЫВ РУКОВОДИТЕЛЯ

на выпускную квалификационную работу студентки

Апальковой Анны Юрьевны

Специальность (направление) 38.03.01 Экономика_____ группа _Б21401бдб

Руководитель ВКР профессор базовой кафедры современного банковского дела,
доктор экономических наук, профессор Л.И. Вотинцева

на тему **Эффективные модели и системы защиты банковской информации: возможности и условия применения на примере ПАО Сбербанк России**

Дата защиты ВКР «_27__» _июня___ 2018 г.

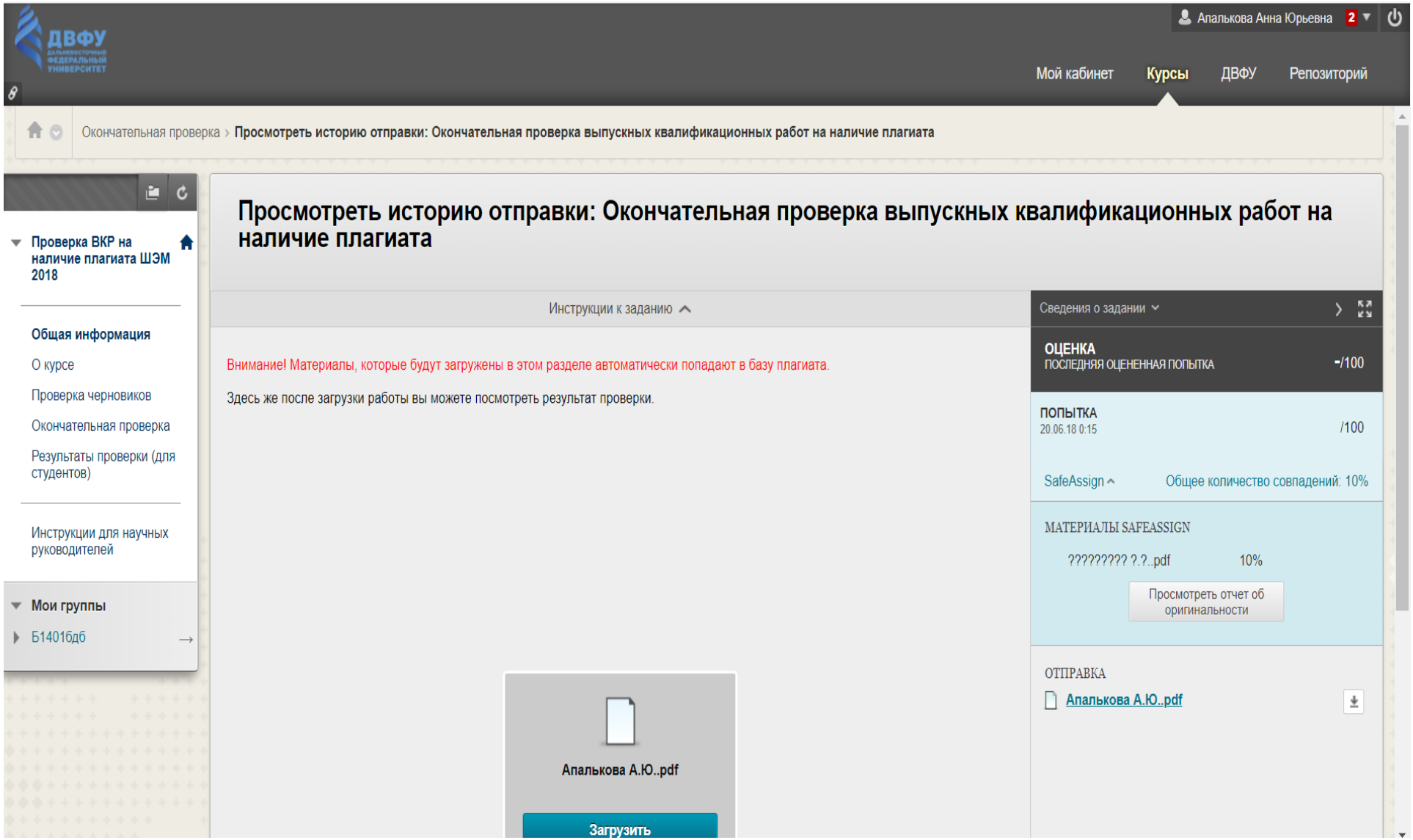
Выпускная квалификационная работа выполнена на актуальную тему в области развития систем защиты банковской информации от не санкционирования проникновения в деловую среду кредитной организации. Работа подготовлена в рамках научного направления кафедры. Результаты исследования практики Сбербанка по созданию препятствий и предупреждений в информационном пространстве операционной деятельности могут использоваться в учебно-методической работе кафедры.

Бакалавр продемонстрировал хорошие способности и умения понимать экономические проблемы, аргументировано и ясно строить письменную речь, обобщать и анализировать деловую банковскую информацию, решать поставленные в ВКР задачи. Степень самостоятельного выполнения работы, ответственности и работоспособности выпускника оценивается на отлично, в границах требования к освоению компетенций, рекомендованных учебным регламентом образовательной программы.

Замечаний по подготовке выпускной работы нет.

Заключение: заслуживает оценки _**отлично**__ и присвоения квалификации _**Бакалавр**.

Руководитель ВКР д.э.н., профессор Л.И.Вотинцева
« 20_»_июня_____2018 г.


ДВФУ
Апалькова Анна Юрьевна
2
Мой кабинет
Курсы
ДВФУ
Репозиторий
Окончательная проверка › Просмотреть историю отправки: Окончательная проверка выпускных квалификационных работ на наличие плагиата
Проверка ВКР на наличие плагиата ШЭМ 2018
Общая информация
О курсе
Проверка черновиков
Окончательная проверка
Результаты проверки (для студентов)
Инструкции для научных руководителей
Мои группы
Б1401бдб
Просмотреть историю отправки: Окончательная проверка выпускных квалификационных работ на наличие плагиата
Инструкции к заданию
Внимание! Материалы, которые будут загружены в этом разделе автоматически попадают в базу плагиата.
Здесь же после загрузки работы вы можете посмотреть результат проверки.
Апалькова А.Ю..pdf
Загрузить
Сведения о задании
ОЦЕНКА
ПОСЛЕДНЯЯ ОЦЕНЕННАЯ ПОПЫТКА
-/100
ПОПЫТКА
20.06.18 0:15
/100
SafeAssign
Общее количество совпадений: 10%
МАТЕРИАЛЫ SAFEASSIGN
????????? ?.?..pdf
10%
Просмотреть отчет об оригинальности
ОТПРАВКА
Апалькова А.Ю..pdf