Содержание

Введение

В настоящее время все большее и большее количество информации окружает нас – все это буквально опутывает человека паутиной информации. Растущие потоки, объемы и скорость поступления, генерирования, хранения и обработки информации обязывают использовать электронные средства – персональные компьютеры. Связанные между собой компьютеры в локальной сети Internet.

Невозможно обеспечить стопроцентный уровень защиты корпоративных информационных систем, при этом корректно расставляя приоритеты в задачах по защите данных в условиях ограниченности доли бюджета, направленной на информационные технологии. Надежная защита вычислительной и сетевой корпоративной инфраструктуры является базовой задачей в области информационной безопасности для любой компании и особенно банковских систем чей уровень доверия состоит из надежности защиты средств и информации клиентов.

Эффективная защита банка в IT сфере и прикладных корпоративных систем сегодня невозможна без внедрения современных технологий контроля сетевого доступа. Участившиеся случаи кражи носителей, содержащих ценную информацию делового характера, все больше заставляют принимать организационные меры, которые будут рассмотрены в дипломной работе на примере ПАО «Сбербанк».

Актуальность темы выпускной квалификационной работы определяется возросшим уровнем проблем информационной безопасности даже в условиях стремительного роста технологий и инструментальной базы для защиты данных.

Предметная область, подлежащая изучению – ПАО «Сбербанк», в частности «кредитование». В сферу этой предметной области попадают

финансово–кредитные учреждения, производящие разнообразные виды операций с деньгами и ценными бумагами. Цель функционирования учреждений этой предметной области – безопасное хранение денег, безналичные переводы от одного клиента к другому, выдача кредитов. Для оказания услуг необходимо наличие квалифицированных специалистов, хранилищ, помещений, удовлетворяющих нормам санитарных и других требований в соответствии с действующим законодательством.

Целью выпускной квалификационной работы это рассмотреть особенности информационной безопасности на предприятии, проанализировать организацию защиты информации в ПАО «Сбербанк».

Поставленная цель обуславливает следующие задачи дипломной работы:

- изучить теоретические аспекты информационной безопасности банка;
- анализ особенностей обеспечения информационной безопасности ПАО «Сбербанк»;
- рассмотреть сущность и содержание информационной безопасности предприятия ПАО «Сбербанк».

1 Анализ предметной области

1.1 Краткая характеристика предприятия

ПАО «Сбербанк» – финансово–кредитное учреждение, производящее разнообразные виды операций с деньгами и ценными бумагами и оказывающее финансовые услуги правительству, юридическим и физическим лицам. (АДРЕС И ФИО ДИРЕКТОРА) Действует на основании специального разрешения (лицензии) полномочных государственных органов. Не имеет права осуществлять производственную, торговую, страховую деятельность.

С 1990 года Центробанку РФ (государству) принадлежит 51% акций Сбербанка, который преобразован в коммерческий банк. Сохранность средств вкладчиков гарантирована государством. Сегодня Сбербанк России является публичным акционерным обществом и находится в статусе крупнейшего коммерческого банка нашей страны. Основным акционером и учредителем Сбербанка России является Центральный банк Российской Федерации, который владеет 50% уставного капитала плюс одна голосующая акция. Другими акционерами Банка являются международные и российские инвесторы.

Обыкновенные и привилегированные акции банка котируются на российских биржевых площадках с 1996 года. Они включены ЗАО «Фондовая биржа ММВБ» в котировальный список первого (высшего) уровня.

Целями и предметом деятельности ПАО «Сбербанк» является:

- привлечение денежных средств от юридических и физических лиц (клиентов) и размещение их на условиях возвратности, платности, срочности;
- осуществление рассчётно–кассового обслуживания клиентов;

- осуществление операций с иностранной валютой и ценными бумагами, иных банковских операций;

- обеспечение сохранности денежных средств, вверенных банку.

ПАО «Сбербанк» выполняет следующие банковские операции и услуги:

- прием, выдачу вкладов и других видов сбережений; – прием платежей от клиентов;

- долгосрочное и краткосрочное кредитование физических и юридических лиц;

- продажу, покупку и управление государственными ценными бумагами;

- реализация лотерейных билетов;

- предоставление клиентам индивидуальных сейфов во временное пользование для хранения документов и ценностей;

- оказание брокерских и консультационных услуг, осуществление лизинговых и трастовых операций;

- приобретение прав требования, вытекающих из поставки товаров и оказания услуг, принятие риска исполнения таких требований и инкассация этих требований (форфейтинг);

- представление интересов предприятий, организаций в финансовых и хозяйственных органах;

- осуществление расчетов по поручениям клиентов, их кассовое обслуживание, а также услуги по инкассации и перевозке денег и ценностей;

- ведение счетов клиентов;

- выдача и оплата, покупка и продажа, хранение платежных документов и ценных бумаг (облигации, чеки, аккредитивы, векселя, акции и т.д.) и иные операции с ними;

- проведение операций по обмену валюты и других валютных операций в установленном Сбербанком порядке;

- выдача гарантий в обеспечение обязательств за третьих лиц, предусматривающих исполнение в денежной форме, в установленном Сбербанком России порядке;
- другие операции по банковскому обслуживанию клиентов в соответствии с лицензией ЦБ РФ и с разрешения Сбербанка.

Управление Сбербанком основывается на принципе корпоративности в соответствии с Кодексом корпоративного управления, утвержденным годовым общим собранием акционеров Банка в июне 2002 года. Все органы управления банком формируются на основании Устава Сбербанка и в соответствии с законодательством Российской Федерации.

Основные направления деятельности Банка:

- кредитование российских предприятий;
- кредитование частных клиентов;
- вложение в государственные ценные бумаги и облигации Банка;
- осуществление операций на комиссионной основе.

Общее собрание акционеров является высшим органом управления ПАО «Сбербанк». На Общем собрании акционеров принимаются решения по основным вопросам деятельности Банка: утверждаются годовые отчеты, принимаются решения о распределении прибыли и выплате дивидендов, утверждается аудитор, избираются члены Наблюдательного совета и Ревизионной комиссии, избирается Президент, Председатель Правления, утверждается новая редакция Устава Банка.

Схема 1.1 – Иерархическая структура банка

В соответствии с Уставом общее руководство деятельностью ПАО «Сбербанк» осуществляет Наблюдательный совет. К компетенции Наблюдательного совета относятся вопросы определения приоритетных направлений деятельности банка, образование коллегиального исполнительного органа – Правления, вопросы созыва и подготовки общих собраний акционеров. В ПАО «Сбербанк» функционирует постоянно действующий коллегиальный рабочий орган – Коллегия Банка, в состав которой входят члены Правления Банка, руководители территориальных и дочерних банков. Коллегия является площадкой для активного обсуждения стратегических вопросов развития банка и выработки оптимальных решений, учитывающих региональные особенности деятельности Банка.

1.2 Особенности системы защиты информации в банковских системах

Особенность системы защиты ПАО «Сбербанк» состоит в организации и функционировании системы безопасности которая соответствовует следующим принципам:

1. Комплексность:

- обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;
- обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;
- способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования банка.

Комплексность достигается:

- обеспечением соответствующего режима и охраны коммерческого банка;
- организацией специального делопроизводства с ориентацией на защиту коммерческих секретов и банковской тайны;
- мероприятиями по подбору и расстановке кадров;
- широким использованием технических средств безопасности и защиты информации;
- развернутой информационно–аналитической и детективной деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно–технических мероприятий.

2. Своевременность – упреждающий характер мер обеспечения безопасности. Своевременность предполагает постановку задач по информационной безопасности на ранних стадиях разработки системы

безопасности на основе анализа и прогнозирование финансовой обстановки, угроз безопасности банка, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3. Непрерывность – считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

- активность. Защищать интересы банка необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

- законность. Предполагает разработку комплексной системы информационной безопасности на основе федерального законодательства в области банковской деятельности, информатизации и защиты информации, частной охранной деятельности и других нормативных актов по информационной безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

- обоснованность. Используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня информационной безопасности и соответствовать установленным требованиям и нормам.

- экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение информационной безопасности (критерий "эффективность – стоимость"). Во всех случаях стоимость системы информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска.

- специализация. Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по

обеспечению информационной безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности банка, его функциональных и обслуживающих подразделений.

- взаимодействие и координация. Означает осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также сотрудничества с заинтересованными объединениями и взаимодействия с органами государственного управления и правоохранительными органами.

- совершенствование. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно–технических требований, достигнутого отечественного и зарубежного опыта.

- централизация управления. Предполагает самостоятельное функционирование системы информационной безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы безопасности разнообразие вариантов построения комплексной системы защиты информации огромное количество, но вот на законном ли основании они составлены и является главным в правовом отношении комплексной системы защиты информации.

1.3 Анализ состояния информационной безопасности

Стратегии информационной защиты для сектора банков довольно сильно отличаются от стратегий компаний и организаций других секторов бизнеса. Это обусловлено прежде всего специфическим характером угроз, а также публичной деятельностью банков, которые вынуждены делать доступ к счетам достаточно легким с целью удобства для клиентов.

Информационная безопасность банка должна учитывать следующие специфические факторы:

- хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги.

На основе информации, содержащейся в банковских компьютерах, производятся выплаты, открываются счета, выдаются кредиты, а также переводятся большие суммы денег. Поэтому ясно, что несанкционированное манипулирование с подобной информацией может повлечь серьезные убытки для клиентов банка. Данная особенность резко расширяет число преступников, совершающих покушения именно на банки.

- информация в банковских системах затрагивает интересы большого количества людей и организаций – клиентов банка.

Как правило, клиенты предоставляют банку

конфиденциальную информацию и потому ожидают, что банк несет ответственность за то, что данная информация находится в строгой секретности. Если банк не выполняет это условие, он рискует своей репутацией со всеми вытекающими отсюда последствиями.

- конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом.

Клиент должен иметь возможность быстро и без утомительных процедур распоряжаться своими денежными средствами. Однако такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

- информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов.

Сбербанк использует современные системы информационной безопасности для обеспечения безопасного и полнофункционального обслуживания клиентов. В 2018 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 2018 год было пресечено более 300 тыс. попыток хищения средств физических и юридических лиц, предотвращен ущерб на сумму более 40 млрд руб.

Сбербанк уделяет особое внимание кибербезопасности. Банк научился успешно противодействовать киберпреступности с помощью интеллектуальной системы защиты клиентов. Проект Сбербанка «Фрод–мониторинг для удаленных каналов обслуживания физических лиц» стал бронзовым призером международного конкурса IPMA International Project Excellence Award 2018. 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.

В 2018 году развитие системы противодействия кибермошенничеству продолжилось, чтобы обеспечить абсолютную защиту всех каналов обслуживания клиентов Сбербанка.

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), с учетом требований федерального законодательства (включая Федеральный закон № 152–ФЗ «О персональных данных» от 27.07.2006) и лучших мировых практик.

При обработке персональных данных банк принимает необходимые правовые, организационные и технические меры для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

В состав мер по обеспечению безопасности персональных данных входят:

- обеспечение контролируемой зоны, в пределах которой осуществляется функционирование автоматизированных систем Сбербанка;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- антивирусная защита;
- обнаружение и предотвращение вторжений;
- контроль и анализ защищенности персональных данных;
- обеспечение целостности автоматизированных систем Сбербанка и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;

- защита технических средств;
- защита автоматизированных систем, их средств, систем связи и передачи данных;
- выявление инцидентов, которые могут привести к сбоям или нарушению функционирования автоматизированных систем и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

В целях нейтрализации актуальных угроз безопасности персональных данных обеспечено применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Доступ к обрабатываемым персональным данным предоставляется только тем работникам Сбербанка, которым он необходим в связи с исполнением ими своих трудовых обязанностей. Все лица, оформляемые на работу в Сбербанк, подписывают обязательства о неразглашении персональных данных и другой конфиденциальной информации, хранение обязательств осуществляется в личных делах работников.

В целях повышения осведомленности, знаний и навыков по вопросам обеспечения информационной безопасности проводится обучение работников в форме обязательного прохождения электронных дистанционных программ подготовки.

Также в Сбербанке организован внутренний контроль (аудит) соответствия обработки персональных данных 152–ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Сбербанка в отношении обработки персональных данных, локальным актам Сбербанка. Внутренний аудит осуществляется Службой внутреннего аудита Сбербанка в рамках аудиторских проверок.

Контроль обеспечения защиты персональных данных при их обработке в автоматизированных системах осуществляется подразделениями Службы кибербезопасности Сбербанка. В рамках реализации мер контроля защищенности информационной инфраструктуры применяются инструментальный контроль защищенности и тестирование на проникновение.

Политика безопасности Сбербанка осуществляется по нескольким элементам:

- нормативно–правового элемент;

В сфере защиты информации ПАО «Сбербанк России» руководствуется следующими нормативно–правовыми актами:

- федеральный закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24–ФЗ;
- закон Российской Федерации «О государственной тайне» (с изменениями от 27 марта 1996 года), принят Верховным Советом Российской Федерации 21.07.93, 5485–1;
- закон Российской Федерации «Об информации, информатизации и защите информации», принят Государственной думой 25.01.95;
- указ Президента Российской Федерации «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» от 3.04.95, 334;
- постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 5.12.91 35;
- постановление Правительства Российской Федерации «Об утверждении правил отнесения сведений, составляющих Государственную тайну, к различным степеням секретности» 870 от 4.09.95;

- указ Президента Российской Федерации «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» от 9.01.96;

- закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных», принят Верховным Советом РФ 23.09.92, 3523–1;

- закон Российской Федерации «О правовой охране топологий интегральных микросхем», принят Верховным Советом РФ 23.09.92, 3526–1;

- указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» 188 от 6.03.97;

- указ Президента Российской Федерации «Об утверждении перечня сведений, отнесенных к государственной тайне» 1203 от 30.11.95;

- указ Президента Российской Федерации «О Межведомственной комиссии по защите государственной тайны» 1108 от 8.11.95;

- постановление Правительства Российской Федерации «О сертификации средств защиты информации» (с изменениями от 23 апреля 1996 года) 608 от 26.06.95;

- федеральный закон «О банках и банковской деятельности» от 25.06.1993 года.

На основе перечисленных документов строится правовая защита информации, призванная обеспечить государственную законодательную базу и нормативное обоснование комплексной системы защиты информации в ПАО «Сбербанк России»

Организационные меры инженерно–технической защиты информации Сбербанка включают в себя, прежде всего, мероприятия по

эффективному использованию технических средств регламентации и управления доступом к защищаемой информации, а также по порядку и режимам работы технических средств защиты информации.

Регламентация предусматривает:

- установку контролируемых границ и охранных зон;
- определение уровней защиты информации в зонах;
- регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т.д.);
- определение режимов работы технических устройств, в том числе сбора, обработки и хранения информации, которая требует защиты, на персональных электронно–вычислительных машинах, передачи документов.

Управление доступом к информации в Сбербанке включает следующие мероприятия:

- идентификацию лиц и обращений;
- проверку полномочий лип и обращений;
- регистрацию обращений к информации, требующей защиты;
- реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений к каналам телекоммуникаций проводится с целью их надежного опознавания.

ПАО «Сбербанк России» использует следующие способы идентификации:

- карточки или ключи;
- пароли и коды;
- в некоторых помещениях установлены биометрические идентификаторы (используются техники цифрового изображения лица в 3D или 2D, отпечатки пальцев и идентификация личности по радужной оболочке глаза).

С помощью биометрических систем безопасности Банк ограничивает или разрешает доступ:

- для сотрудников – в служебные помещения банка (касса, серверная, бухгалтерия, кабинеты руководства); в депозитарий для клиентов;
- для клиента – к своей ячейке;
- для особо важных клиентов – в ряд специальных помещений.

При этом биометрия существенно понижает вероятность проникновения нежелательной личности в зону с ограниченным доступом, создает психологический барьер для потенциального злоумышленника, а также документально подтверждает факт прохода в охраняемые помещения каждой личности.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

Реагирование на любое обращение к информации заключается либо в разрешении доступа к информации, либо в отказе. Отказ может сопровождаться включением сигнализации, оповещением службы безопасности или правоохранительных органов, задержанием злоумышленника при его попытке несанкционированного доступа к защищаемой информации.

В системе безопасности Сбербанка применяются специальные средства видеоконтроля. Сетевой программно–аппаратный комплекс видеоконтроля и автоматизированного управления интегрированными системами безопасности «Инспектор+» сочетает в себе высокое качество компьютерных цифровых технологий с возможностью

объединения автономных компонентов системы безопасности банка в профессиональную интегрированную систему безопасности. «Инспектор+» позволяет распределить приоритеты между видеоканалами таким образом, что в момент тревоги тревожной камере выделяется максимальный ресурс по скорости записи, который даже в режиме мультиплексирования составляет до 10–12,5 FPS. Помимо качественного видеоконтроля «Инспектор+» осуществляет синхронно с видеоконтролем аудио контроль.

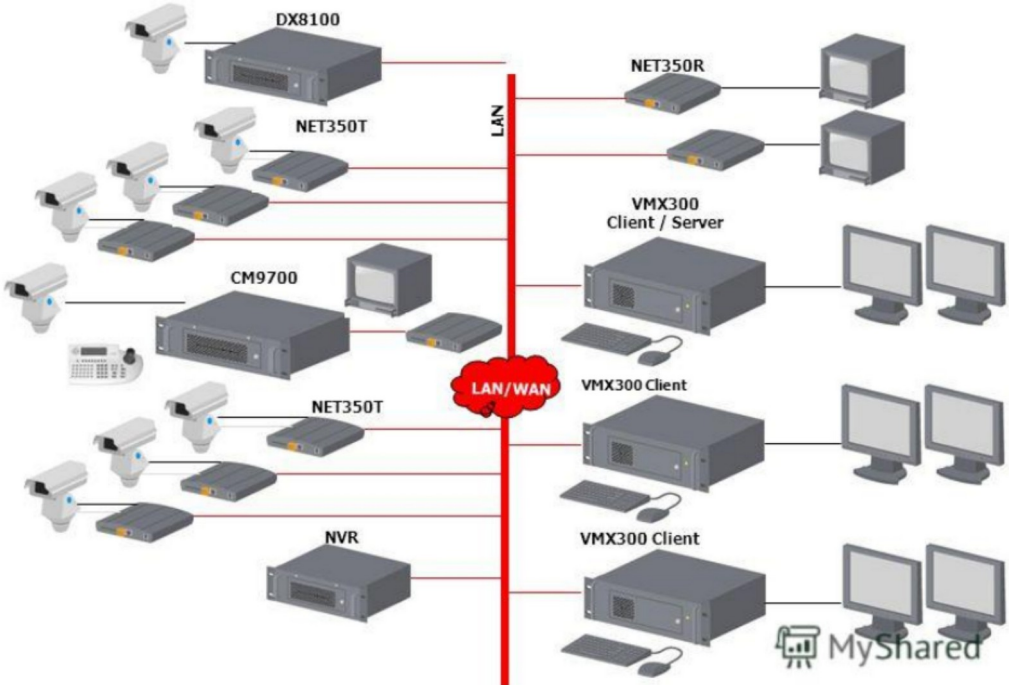


Рисунок 1.3.1 – «Инспектор+»

Объединение сети банка в единое пространство безопасности в технологии «Инспектор+» происходит через видео шлюз, который призван сопрягать высокоскоростные характеристики локальных сетей с медленной работой межсетевых соединений.

Помимо видео шлюза, в арсенале технологии «Инспектор+» содержатся и другие полезные модули.

Модуль резервного копирования, или видео архивации, – это объект, управляющий процессами архивации видеоданных. Модуль видео архивации позволяет создавать централизованный архив

видеоданных. Как правило, данная функция используется при решении задач долговременного хранения большого объема информации или информации, имеющей стратегическое значение.

Модуль телеметрического управления используется для дистанционного управления камерами, установленными на двухкоординатных поворотных устройствах. Управление всеми камерами может осуществляться как с любой клавиатуры, так и посредством управляющих окон на экране компьютера.

Для защиты банкоматов в технологии «Инспектор+» существует подсистема «Банкомат Инспектор». Данная подсистема позволяет создать интегрированную систему защиты требуемой конфигурации как для одного банкомата, так и для территориально– распределенной сети банкоматов, что является наиболее сложной задачей, которую невозможно решить обычными средствами обеспечения безопасности. В системе «Банкомат Инспектор» полностью интегрированы устройства видеонаблюдения, сенсоры и оборудование передачи сигналов с возможностью гибкой настройки логики системных реакций на входные события.

2 Разработка комплекса мер по обеспечению защиты информации

С учетом проведенной оценки киберугроз и возможных рисков выполняется анализ программно–технических средств защиты, прорабатывается архитектура решений для обеспечения информационной безопасности.

Для минимизации зависимости от продукции одного вендора, устанавливаемой на серверы, рабочие станции и сетевые шлюзы, рекомендуется использовать средства защиты нескольких производителей для различных сегментов инфраструктуры организации.

В настоящее время можно выделить следующие классы решений по защите от проникновения вредоносного ПО:

Комплексная защита рабочей станции, включающая классический антивирус, расширенные технологии безопасности (персональный межсетевой экран, система предотвращения вторжений, контроль приложений, управление съёмными носителями и др.) и инструменты расследования и восстановления.

Антивирусные решения, реализующие защиту от вредоносного ПО на конечных устройствах – рабочих станциях, серверах, мобильных устройствах – осуществляют детектирование преимущественно методом сигнатурного и эвристического анализа.

Песочницы представляют собой изолированную виртуальную среду для безопасного запуска и анализа поведения непроверенного кода. Многие современные вредоносные программы имеют функции анти–детектирования и не проявляют себя в случае обнаружения эмуляции среды запуска. Поэтому в песочницах выполняется анализ непроверенного кода в операционных средах с различными конфигурациями, характеристиками и наборами открытых уязвимостей.

Песочницы используются для обнаружения не известных ранее вирусов, не детектируемых методом сигнатурного анализа.

Anti–APT решения позволяют обнаружить атаки «нулевого дня», выявить факты проникновения в сеть, сетевые аномалии и подозрительное поведение устройств, детектируют атаки на Active Directory и горизонтальные перемещения злоумышленника в инфраструктуре организации. Решения для выявления и предотвращения целевых атак анализируют сетевой трафик, используя сигнатурный и поведенческий анализ, а также выявляют угрозы на сетевом уровне.

Технология сочетает в себе непрерывный мониторинг и сбор данных о конечных точках в режиме реального времени. EDR–системы обнаруживают признаки вторжения, анализируя отклонения в поведении приложений, формируют ответ на атаку, централизованно собирают данные для мониторинга состояния конечных устройств и расследования инцидентов, анализируют сведения об источнике угрозы и выполняют проактивный поиск угроз.

Системы UEBA анализируют журналы конечных устройств и сетевого оборудования, оценивают данные систем аутентификации, строят модели поведения пользователей (UBA) и ИТ–объектов, выявляют отклонения.

Системы XDR выполняют расширенное обнаружение и автоматизированное реагирование на сложные угрозы и целевые атаки, представляют собой комплексное многомодульное решение одного вендора, обогащенное данными о киберугрозах.

Системы XDR функционирует в составе минимального набора модулей защиты:

- конечных точек;
- сети;
- почтового трафика;
- веб трафика.
- Сенсорами XDR могут быть:

- EPP;
- EDR;
- почтовый шлюз;
- шлюз web–трафика;
- NTA/NTDR;
- IDM и др.

Автоматизированное реагирование на кибератаки позволяет снизить время реагирования на инцидент и принятие решения. Многомодульность систем XDR позволяет учитывать комплексный подход злоумышленников к проникновению в организацию, при котором атаке одновременно подвергаются различные элементы инфраструктуры.

SOAR–системы анализируют события кибербезопасности, централизованно собранные сенсорами разных вендоров, выявляют инциденты и реагируют на них согласно заданному алгоритму. Также они автоматизируют операции реагирования на инциденты и расследование.

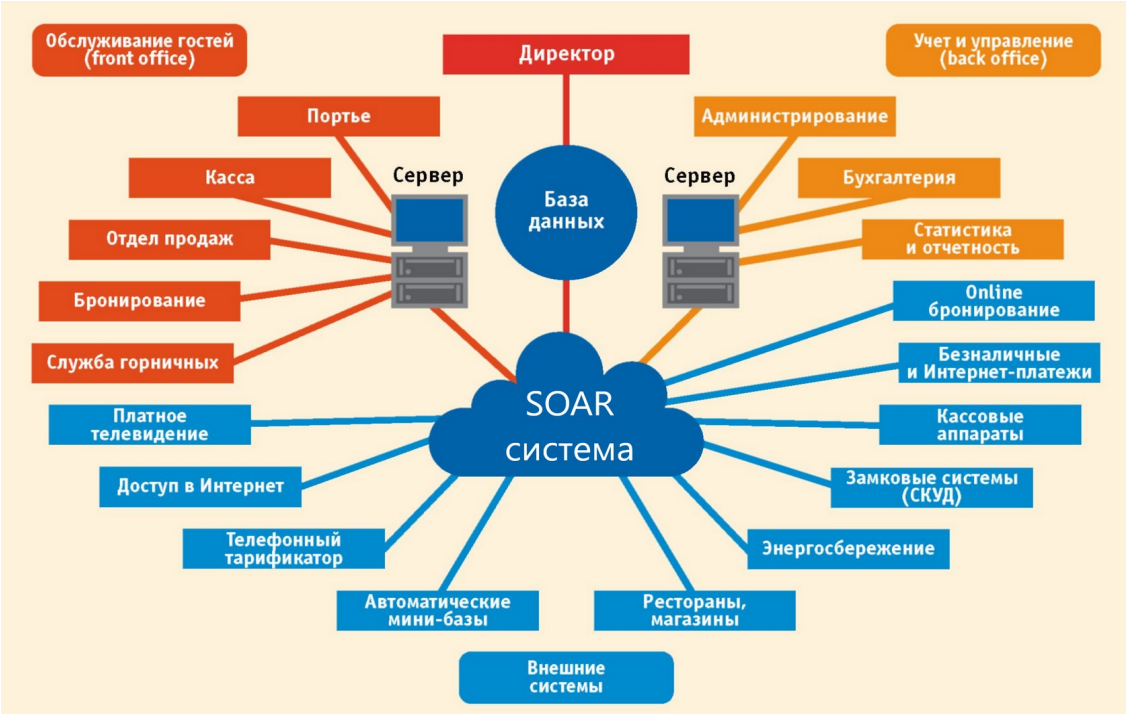


Рисунок 2.1 – SOAR–системы

Системы обнаружения и предотвращения вторжений анализируют данные и сетевое поведение для отслеживания несанкционированной вирусной активности и на основании анализа трафика выявляют угрозы кибербезопасности.

IPS/IDS используют анализаторы, основанные на правилах, сигнатурах и обнаружении аномалий. Данные решения могут анализировать зашифрованный трафик.

Критически важной мерой защиты от кибератак и заражения вредоносным ПО является регулярное обновление программных и программно–технических средств защиты.

Эффективным способом обновления будет использование облачных механизмов обновлений сигнатурных баз и правил (если это приемлемо для организации).

Профилирование средств защиты должно осуществляться компетентными специалистами для исключения ошибок конфигурирования средств защиты и настройки политик.

По результатам регулярного анализа киберугроз должен выполняться контроль корректности и корректировка настроек конфигурации средств защиты.

Настройка фильтрации пакетов данных на межсетевых экранах конечных устройств предназначена для защиты корпоративной инфраструктуры от возможных вирусных сетевых атак. Должна обеспечиваться корректная фильтрация на канальном, сетевом, транспортном и прикладном уровнях модели OSI.

Необходимо проработать вопросы, связанные с применением, настройкой и контролем безопасности применяемых технологий и программного окружения. Например, обеспечить использование только безопасных протоколов, отключить загрузку активного содержимого в браузерах конечных устройств. Также нужно включить

защиту cookie, рассмотреть возможность запрета включения макросов в офисном ПО, настроить защиту загрузочного сектора устройств, ограничить перечень загрузочных устройств и т.д.

Необходимо обеспечить контроль подключения внешних устройств и ограничить использование интерфейсов подключения в соответствии с принципом минимальных привилегий.

Должна выполняться антивирусная проверка файлов, размещенных на подключаемых съемных носителях.

Для обеспечения безопасной работы пользователей в интернете доступ к вредоносным web–ресурсам должен быть запрещен. Настроить данное ограничение можно, используя системы защищенного интернет–доступа.

Мера позволит защитить внутренние сегменты сети от проникновения вредоносного ПО при работе пользователя с внешними сайтами.

Необходимо реализовать управление доступом пользователей к ресурсам компании и обеспечить безопасные административные интерфейсы для управления инфраструктурой и программным окружением организации: обеспечить применение парольной политики с целью использования стойких паролей, использовать многофакторную аутентификацию, контролировать блокировку неиспользуемых учетных записей, а также использование технологических учетных записей.

С учетом вышеописанных мер защиты необходимо провести разработку сценариев реагирования на инциденты, реализовать мониторинг и оперативный ответ на ИБ–события.

Это позволит своевременно обнаружить, локализовать и блокировать вирусную атаку, устранить выявленные уязвимости, минимизировать ущерб от реализации киберугрозы, ликвидировать последствия и предотвратить повторные кибератаки.

При реализации мер защиты необходимо помнить о важной категории киберугроз – человеческом факторе. Ошибочные действия пользователей часто приводят к реализации вирусных атак.

Для минимизации киберрисков и возможного ущерба необходимо применять следующие организационные меры:

Обучение сотрудников правилам кибергигиены и противодействия вирусным атакам является неотъемлемой частью обеспечения информационной безопасности. Особое внимание стоит уделить темам безопасной работы с корпоративной электронной почтой, правилам реагирования на обнаружение вредоносного ПО, способам выявления фишинга, описанию методов социальной инженерии, правилам обращения с собственными и «случайно» найденными внешними носителями. Сотрудникам необходимо предоставить способ оперативно связаться с подразделениями кибербезопасности в случае появления любых подозрений на нелегитимную деятельность внутри организации.

Персонал организации должен быть ознакомлен с требованиями кибербезопасности и политикой информационной безопасности, включающей требования к антивирусной защите.

В организации должны быть разработаны меры обеспечения защиты от вредоносного ПО:

- политика информационной безопасности организации (включая требования к антивирусной защите);
- инструкции и регламенты работы пользователей;
- политика антивирусной безопасности;
- описание процедур, обеспечивающих процесс эксплуатации систем антивирусной безопасности.

2.1 Организационные меры обеспечения политики информационной безопасности

Организация мер политики безопасности ПАО « Сбербанк» начинается с правовой формы защиты информации – это защита информации склонно на применении Гражданского и Уголовного кодексов, Федеральных законов и других нормативно–правовых актов, регулирующих деятельность в области информатики, информационных отношений и защиты информации.

Настоящая Концепция базируется на следующих нормативно–правовых актах:

- «Гражданский кодекс Российской Федерации» от 30.11.94 г., №151–ФЗ ч.1, ст. 139;
- «Уголовный Кодекс Российской Федерации» от 13.06.96г., №63–ФЗ ст. 183, 272, 273, 274;
- «Гражданский кодекс Российской Федерации» от 21.01.96 г., №14–ФЗ ч.2, ст. 857;
- «Трудовой кодекс Российской Федерации» от 30.12.01, №197–ФЗ ст. 85,86,87,88,89,90;
- Федеральный Закон Российской Федерации «О банках и банковской деятельности» от 02.12.90г. №395–1, ст.26;
- «Кодекс Российской Федерации об административных правонарушениях» от 30.12.01, №195–ФЗ ст. 13.12, 13.13, 13.14;
- Федеральный Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149–ФЗ;
- Федеральный закон «О лицензировании отдельных видов деятельности» от 08.08.2001 №128–ФЗ (в ред. от 21.03.2002 № 31–ФЗ);
- Указ Президента РФ от 06.03.97г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

- Постановление Правительства РФ от 15.08.06. №504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Приказ ФАПСИ от 13.06.01г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Гражданский кодекс РФ и Закон «Об информации, информационных технологиях и о защите информации» позволяют рассматривать информацию как специфический объект права. Закон выделяет три категории информации:

- информация, составляющая государственную тайну;
- информация, составляющая коммерческую тайну;
- персональные данные.

Предметом рассмотрения данной Концепции является информация второй и третьей категорий. Банк в процессе своей деятельности выступает не только собственником, но и пользователем информации, доверенной ему клиентами, контрагентами или сотрудниками. Банк вправе распоряжаться такой информацией, следовательно и выбирать степень её защиты.

Решение задач правового обеспечения информационной безопасности Банка достигается формированием системы внутренних инструкций, положений, планов, правил.

Работа по обеспечению информационной безопасности в Банке включает следующие этапы:

- определение информации, содержащей коммерческую тайну, и сроков ее действия;

- категорирование помещений по степени важности обрабатываемой в них информации;
- определение категории информации, обрабатываемой каждой отдельной системой;
- выбор средств и мер защиты для предотвращения воздействия факторов риска и их минимизации;
- описание системы, определение факторов риска, определение уязвимых мест систем;
- выбор средств и мер контроля и управления для своевременной локализации и минимизации воздействия факторов риска.

Отнесение информации к коммерческой тайне – это установление ограничений на распространение информации, требующей защиты. Среди сведений относимых к категории коммерческой тайны применительно к банку, можно выделить следующие: деловую информацию о деятельности банка, финансовую документацию, различные сведения о клиентах, партнерах, сметы, отчёты, перспективные планы развития, аналитические материалы, исследования и т.п.

Отнесение информации к коммерческой тайне осуществляется в соответствии с принципами законности, обоснованности и своевременности. Обоснованность отнесения информации к коммерческой тайне заключается в установлении путем экспертной оценки целесообразности защиты конкретных сведений исходя из жизненно – важных интересов Банка, вероятных финансовых и иных последствий нарушения режима соблюдения коммерческой тайны. Своевременность отнесения сведений к коммерческой тайне заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Чтобы отнесение информации к категории коммерческой тайны приобрело законную силу, оно должно быть оформлено в виде

специального «Перечня сведений, составляющих коммерческую тайну МОРСКОГО АКЦИОНЕРНОГО БАНКА» (Открытое Акционерное общество) (далее Перечень), который разрабатывается (уточняется не реже одного раза в год) постоянно действующей Комиссией Банка по защите коммерческой тайны, назначаемой приказом Председателя Правления Банка.

Перечень разрабатывается путем экспертных оценок на основании предложений подразделений Банка и с учетом действующего законодательства. В Перечне указываются категории сведений, их степень конфиденциальности, срок действия ограничений на доступ к ним. Перечень утверждается Председателем Правления Банка.

Степень конфиденциальности информации, составляющей коммерческую тайну, должна соответствовать степени тяжести ущерба от происшествие, который может быть нанесен безопасности Банка вследствие её распространения. В соответствии с этим среди информации, относимой к коммерческой тайне, выделяются две группы: информация общего характера и информация, доступ к которой должен носить исключительный характер.

Такой информации отдельно присваивается гриф «Конфиденциально». Присвоение грифа «Конфиденциально» или его отмена принадлежит Председателю Правления Банка.

Категорирование помещений производится по степени важности обрабатываемой в них информации. В зависимости от категории обрабатываемой информации принимаются соответствующие меры по защите помещений.

Для каждой информационно–вычислительной системы Банка, а в отдельных случаях для персональных компьютеров (ПК), определяется категория обрабатываемой в ней информации с учетом «Перечня сведений, составляющих коммерческую тайну Банка». В зависимости от

категории обрабатываемой информации принимаются соответствующие меры по ее защите в системе.

Основная задача этапа описания систем – описание защищаемого периметра, т.е. определение средств и непосредственных данных, подлежащих защите. В описание системы включаются:

- цели и задачи системы;
- пользователи и обслуживающий персонал;
- способы взаимодействия с другими системами как внутри Банка, так и с внешними объектами;
- физическую топологию сети в зданиях Банка;
- логическую топологию сети Банка, ее основные характеристики;
- перечень используемого оборудования, включая коммуникационное, периферийное, серверы, ПК, оборудование, их основные характеристики;
- перечень используемого программного обеспечения (системное, прикладное, коммуникационное) и их характеристики.

Описание системы должно проводиться с учетом организационной структуры подразделений, которые будут ее эксплуатировать.

Факторы риска — это возможные ситуации, возникновение которых может расцениваться как угроза, и способные нанести ущерб материального или нематериального (морального) характера. Фактор риска оказывает воздействие на определенные участки объектов информационной безопасности и может учитываться или не учитываться в зависимости от степени воздействия на жизнедеятельность Банка. Основными факторами риска являются:

- стихийные бедствия или чрезвычайные ситуации, приводящие к полному или частичному выходу из строя технических средств систем;
- несанкционированный доступ к серверам, элементам аппаратуры и оборудованию в серверных комнатах;

- неисправности и нарушения в функционировании программных и технических средств, отказ в санкционировании доступа к оборудованию, программам и данным, вызванные случайными сбоями или отказами;
- несанкционированные проникновения в информационно–вычислительную систему, в том числе по внешним каналам связи;
- мошенничество или умысел, а также некомпетентность или халатность, которые приводят к нарушению целостности или доступности информации;
- нарушение конфиденциальности отдельных данных;
- повторное использование внешних и внутренних носителей информации для съема информации;
- несанкционированный доступ к системным и прикладным данным и программам, а также ресурсам систем;
- нарушение конфиденциальности массивов данных.

Перечень факторов риска может уточняться.

Уязвимые места – элементы технических средств, программ и данных, которые могут быть подвергнуты воздействию факторов риска. Уязвимые места необходимо защищать и контролировать. К уязвимым местам объектов информационной безопасности относятся:

- все технические средства – необходимо защищать от стихийных бедствий, диверсий, несанкционированного доступа (НСД), сбоев и отказов;
- все системное программное обеспечение и системные ресурсы, обеспечивающие функционирование автоматизированных систем и сетей Банка – необходимо защищать от НСД, приводящего к нарушению целостности и доступности;
- все автоматизированные рабочие места (АРМ) и терминалы – необходимо защищать от НСД;

- опорная сеть Банка и передаваемые по ней данные – необходимо защищать от нарушения целостности или доступности и НСД;
- ресурсы и приложения систем, внутренние и внешние носители информации в системах, обрабатывающих конфиденциальную информацию – необходимо защищать от повторного использования («сборки мусора»);
- конфиденциальная и строго конфиденциальная информация – необходимо защищать от нарушения конфиденциальности;
- помещения, слаботочное оборудование, вычислительная техника подсистем, на которых обрабатывается конфиденциальная информация – необходимо защищать от перехвата информации по каналам электромагнитного излучения и закладных устройств.

Перечень уязвимых мест системы Банка может уточняться. Для каждого конкретного объекта информационной безопасности осуществляется выбор конкретных средств и методов защиты, контроля и управления с учетом уязвимых мест и факторов риска.

2.2 Обоснование методов и средств обеспечения информационной безопасности

ПАО «Сбербанк» являясь государственным банком, находящимся в пользовании миллионами россиян, нуждается в надежной защите, которая состоит из двух этапов:

- внешняя политика безопасности;
- внутренняя политика безопасности.

Во внешнюю политику входят такие виды защиты как:

- забор (с колючей проволокой);
- пост охраны на входе в банк. Нужны для быстрого реагирования препятствия побегу злоумышленника и других опасных лиц;
- ключ карты и FLASH–носители электронных ключей. Ключ карты используют для входа в кабинеты с ограниченным доступом, а электронные ключи во FLASH–носителе нужны для входа в систему;
- охрана банка. Осуществляет мониторинг камер, быстрое реагирование на сомнительных или опасных лиц или злоумышленников;
- системы слежения и т. д.

Внутренняя политика безопасности ПАО «Сбербанка» имеет более обширный спектр различных угроз и для защиты используют такие организации как ПАО «Сбербанк» используют локальную, корпоративную сеть со строгой групповой политикой и в штатном режиме используется анти–вирус «Kaspersky», а для глобальной защиты информационных систем ПАО «Сбербанк» и подобные масштабам организации заказывают индивидуальное ПО которое имеет статус коммерческой тайны.

Для технического обеспечения у ПАО «Сбербанк» существует дочерняя компания СберСервис, которая осуществляет техническое обслуживание компьютерных систем, банкоматов, терминалов, прокладкой кабелей сетей и т. д.

ПАО сбербанк позаботился о собственной защите сформировав внутреннюю и внешнюю защиту, составил групповую политику, обеспечил организацию индивидуальной антивирусной защитой и нанял целый штат IT сотрудников для технического и программного обслуживания, осталось забота о своих клиентах и вкладчиках.

Защита клиентов ПАО «Сбербанк» обеспечивается работой центра фрод–мониторинга, который заботится о клиентах и при проведении любых нестандартных операций связывается с клиентом, и мы во многом не допускаем мошеннических действий со стороны киберпреступников.

К сожалению, есть тренд на увеличение попыток атаковать клиентов банка с использованием методов социальной инженерии, когда мошенники пытаются обманным путем завладеть чувствительной информацией в виде паролей, ключевых слов либо персональными данными, чтобы воровать деньги со счетов. Эффективность центра фрод–мониторинга достигла одного из лучших показателей в мире, и около 97% операций, которые являются мошенническими, мы умеем хеджировать и не допускать совершения преступления.

IT команда ПАО «Сбербанка» – это в том числе объект внимания кибер–мошенников для получения какой–то чувствительной информации или попыток преодолеть барьеры для доступа в наши системы. Поэтому банк внедряет принципы кибер–культуры, регулярно проводим учения среди сотрудников, ведем разъяснительную работу – как управлять личными кибер–рисками, своими паролями.

ПАО «Сбербанк» использует весь передовой международный опыт. Был создан Операционный центр кибербезопасности, так называемый Security Operation Center, который в круглосуточном режиме

мониторит все киберугрозы вокруг систем Сбербанка. Сбербанк к концу прошлого года стал первым российским банком, получившим сертификат соответствия международному стандарту по информационной безопасности от Британского института стандартов – BSI, он же и аудировал работу наших систем. Для нас это очень важно, потому что очень важно жить по стандартам, которые существуют в мире.

2.3 Определение мест размещения средств обеспечения информационной безопасности

Согласно плану помещения ПАО «Сбербанк», разработаем план расположения всех компьютеров и средств защиты информации.

Для защиты конфиденциальных сведений, циркулирующих в средствах обработки, хранения, и передачи информации от утечки по техническим канала в ПАО «Сбербанк» следует применить следующие средства:

- укрепленное стекло шпион;
- генератор шума;
- камера слежения;
- датчик движения;
- подавитель диктофона;
- электронный замок;
- огнетушитель;
- датчик дыма.

Так же для предотвращения утечки информации по оптическим каналам необходимо расположить ЭВМ в кабинете отдела технической защиты информации таким образом, чтобы нельзя было просматривать с двери.

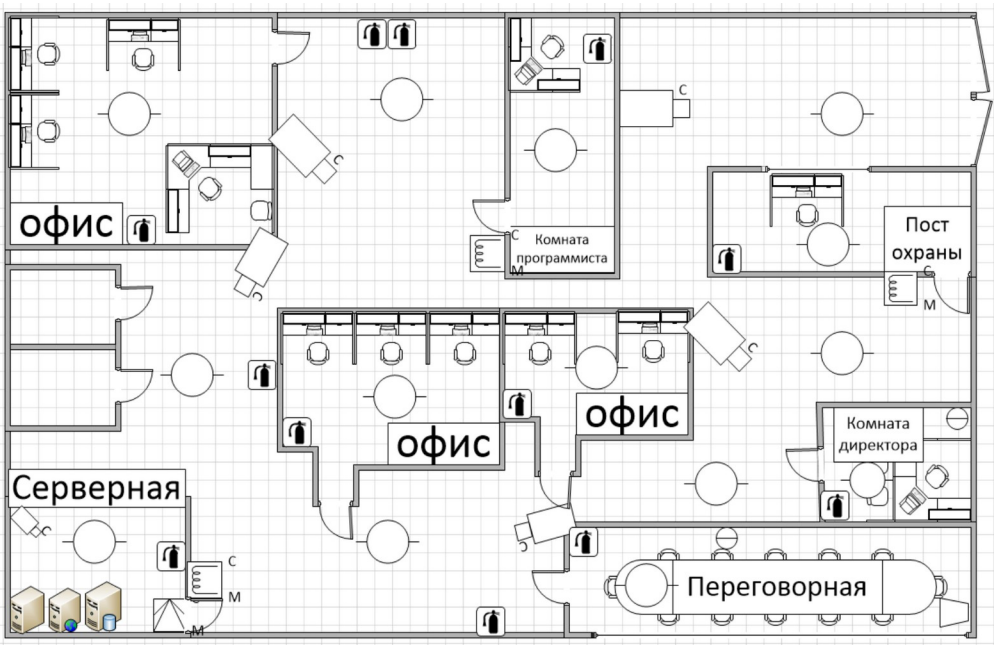
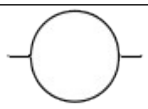
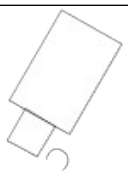
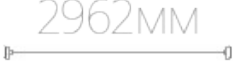


Рисунок 2.3.1 – Расположение всех средств защиты

Таблица 2.3.1 – Обозначение средств защиты

	Датчик дыма
	Камера слежения
	Огнетушитель
	Электронный замок
	Датчик движения
	Подавитель диктофона
	Генератор шума
	Зеркало шпион (Гизелла), укрепленное

Тканевые жалюзи помогают исключить утечку данных по оптическим каналам. Так же для защиты от утечек по оптическим каналам следует так располагать ПК, чтобы не было отражения света. Если отражение света от технических средств будет присутствовать, то тогда вероятна утечка информации. Следует вводить ограничения на освещения.

Доводчик двери позволяет защитить помещение от прямого съёма информации. Тем самым данные меры защиты должны исключить основные каналы утечки информации.

Выбор оборудования от утечек требует тщательного подбора. Основная задача таких средств – это защита конфиденциальной информации. Для решения задач по безопасности информационного пространства следует проанализировать вероятные угрозы.

Основными угрозы:

- утечка информации по каналам ПЭМИН;
- закладные устройства;
- утечка по оптическому каналу;
- утечка при прямом воздействии (кража данных с ПК или с носителя).

Любая из этих угроз приводит к потере данных, а следовательно, и к финансовым потерям. Утечка информации по ПЭМИН обычно осуществляется с помощью съёма побочных опасных сигналов, которые несут в себе информацию. Перехват данных ведётся дистанционно, для предотвращения таких утечек используют специальные комплексы или так называемые генераторы шумов. Они маскируют сигнал, который при перехвате изменяется в параметрах. Это приводит к тому, что данные теряют свою ценность и актуальность.

Существуют много генераторов шумов, но из большого количества следует выбрать тот генератор, который подходит по

финансовым критериям. Так же генератор шума должно качественно выполнять функцию маскирования опасных излучений. При выборе следует учитывать такие характеристики, как габариты устройства, диапазон частот и сертификат качества.

"КАНОНИР–К7" – подавитель диктофонов и подслушивающих устройств. Подавитель «КАНОНИР–К7» предназначен для защиты места переговоров от средств съёма акустической информации. В бесшумном режиме блокируются радио микрофоны, проводные микрофоны и большинство профессиональных цифровых диктофонов и диктофонов в мобильных телефонах (смартфонах).

Рисунок 2.3.2 – "КАНОНИР–К7"

БУБЕН это – изделие используется при проведении конфиденциальности переговоров для создания акустических помех в замкнутом помещении. Изделие может работать в любом из двух режимов:

- формирование речеподобной помехи,
- формирование помехи типа «белый шум».

Рисунок 2.3.3 – Генератор шума БУБЕН

2.4 Комплекс программно–аппаратных средств обеспечения информационной безопасности

Система защиты информации ПАО «Сбербанк» – это комплекс мер, а также соответствующих им мероприятий, сил, средств и методов. Программно–аппаратный компонент системы защиты информации предназначен для защиты данных, обрабатываемых и хранящихся в компьютерах и серверах локальных сетей в различных информационных системах. Как правило, он реализует тесно взаимосвязанные процессы:

- управление доступом и управление политикой безопасности,
- идентификацию и аутентификацию пользователей,
- регистрацию событий и аудит,
- криптографическую защиту,
- сетевую защиту,
- антивирусную защиту,
- обнаружение атак программными средствами (IDS – Intrusion Detection Systems).

Средства управления доступом позволяют разграничивать и контролировать выполняемые над информацией действия, которые совершаются пользователями (ограничение доступа на вход в систему, разграничение доступа авторизованных пользователей, запрет доступа неавторизованных пользователей и т.п.). То есть речь идет о логическом управлении доступом, который реализуется программными средствами. Контроль прав доступа осуществляется посредством различных компонентов программной среды – ядром сетевой операционной системы, системой управления базами данных, дополнительным программным обеспечением и т.д.

Идентификация предназначена для того, чтобы пользователь мог идентифицировать себя путем сообщения своего имени. С помощью

аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в систему, действительно тот, за кого себя выдает.

Регистрация событий (протоколирование, журналирование) – это процесс сбора и накопления информации о событиях, происходящих в информационной системе. Возможные события принято делить на две группы:

- внешние события, вызванные действиями как авторизованных, так и неавторизованных пользователей;
- внутренние события, вызванные действиями пользователей и администраторов, аудитом называется процедура анализа накопленной в результате журналирования информации, этот анализ может осуществляться оперативно, почти в реальном времени, или периодически.

Методы криптографии – одно из наиболее мощных средств обеспечения конфиденциальности и целостности информации. Как уже упоминалось, основной элемент криптографии – шифрование.

Сетевая защита, как правило, обеспечивается установкой на границе сетей так называемых экранов. Экран – это средство разграничения доступа пользователей из одного сетевого множества к ресурсам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем. Примерами экранов являются межсетевые экраны, устанавливаемые для защиты локальной сети организации, имеющей выход в публичную сеть (такую как Интернет).

Помимо прочего, сегодня практически все производители программно–аппаратных средств обеспечения безопасности информации включают поддержку антивирусной защиты и систем обнаружения вторжений, обеспечивающих защиту от вредоносного ПО и атак.

Для примера приведем аппаратные межсетевые экраны D–Link серии DFL, обладающие функцией проверки трафика на наличие вредоносных программ. В частности, даже "младшая" модель DFL–260/260E позволяет сканировать на наличие вредоносного ПО файлы любого размера, используя технологию потокового сканирования. Данный метод сканирования увеличивает производительность проверки, сокращая так называемые "узкие места" в сети. Межсетевые экраны серии DFL используют сигнатуры вирусов от антивирусной компании "Лаборатории Касперского" (Kaspersky Labs). При этом существует возможность обновления сигнатур. В результате вирусы и вредоносные программы могут быть эффективно заблокированы до того, как они достигнут устройств локальной сети.

Кроме того, для эффективной борьбы с вредоносным трафиком и для того, чтобы минимизировать влияние аварийной ситуации на всю сеть, межсетевые экраны компании D–Link (DFL–800/860/860E/1600/1660/2500/2560) поддерживают специальную функцию – ZoneDefense, представляющую собой механизм, позволяющий им работать с коммутаторами локальных сетей D–Link и обеспечивающий активную сетевую безопасность. Функция ZoneDefense автоматически изолирует инфицированные компьютеры локальной сети и предотвращает распространение ими вредоносного трафика. Более подробно аппаратные межсетевые экраны компании D–Link и о технологии ZoneDefense мы рассмотрим в следующих главах.

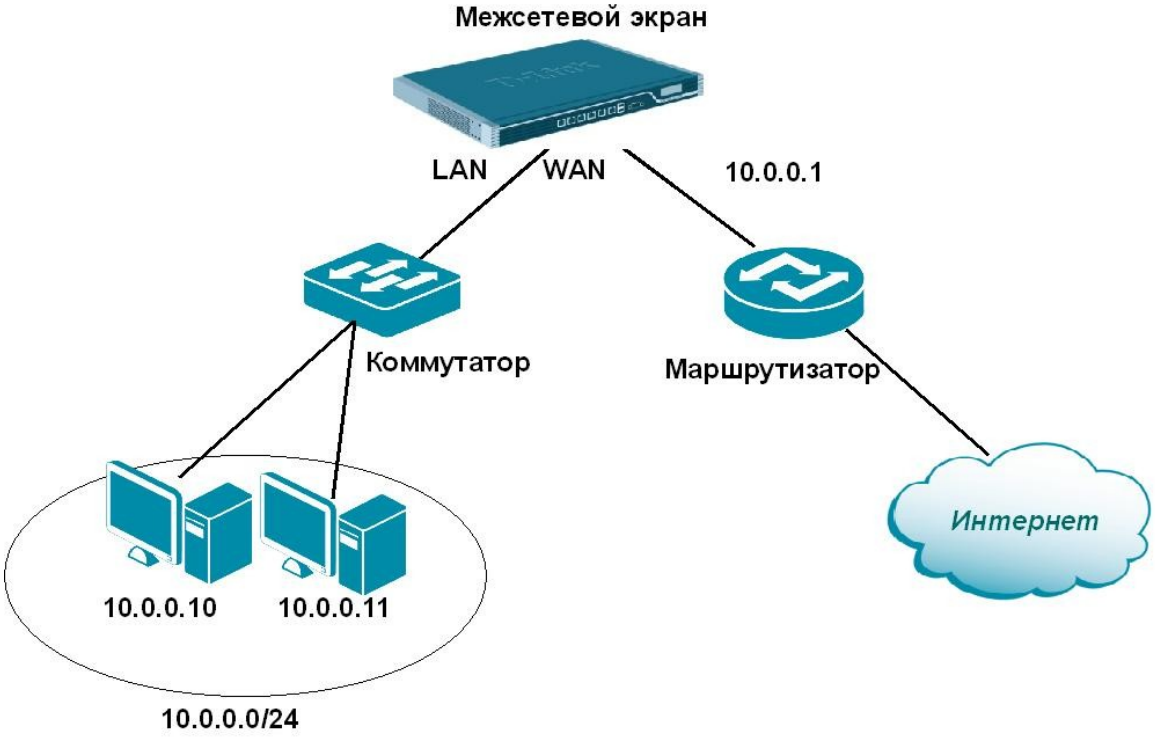


Рисунок 2.4.1 – межсетевой экран NetDefend для сетей SOHO

3 Оценка эффективности предлагаемых мероприятий

В настоящее время стало необходимым наличие в каждом банке «Политики информационной безопасности банка», главного документа при формировании системы его информационной безопасности. В данном документе выделяются серьезные угрозы безопасности информации в банке, представляется описание объектов защиты, устанавливаются ключевые задачи информационной безопасности, а также меры по обеспечению информационной безопасности банковской системы.

Главными элементами системы информационной безопасности банка являются:

- авторизация и аутентификация;
- защита от несанкционированного доступа к системам, в том числе и внутренняя защита от незаконного доступа сотрудников банка;
- защита каналов передачи данных, обеспечение целостности и актуальности данных при обмене информацией с клиентами;
- обеспечение юридической значимости электронных документов; - управление инцидентами информационной безопасности;
- управление непрерывностью ведения бизнеса;
- внутренний и внешний аудит системы информационной безопасности.

При формировании системы информационной безопасности банка следует учесть и такие функциональные требования к системе:

- получение от должностных лиц в зависимости от их иерархической подчиненности той информации, которая необходима им для решения поставленных задач;
- возможность использования должностными лицами всего арсенала средств математического и программного обеспечения в интересах принятия решений;

- обеспечение диалогового взаимодействия участников при работе с системой;

- соответствие процессов функционирования и применения системы методам и логике деятельности должностных лиц;

- соответствие особенностей хранения информации свойствам ее источников и потребителей, обеспечение требуемой срочности, периодичности и очередности ее представления;

- возможность объективного контроля и проверки промежуточных данных и результатов на основе протоколирования.

Долгосрочное адекватное функционирование системы информационной безопасности способно обеспечить только систематическое поддержание баланса между всеми составляющими системы и элементами ее окружения. Такое соответствие является основной задачей поддержания информационной безопасности в банковской деятельности.

Одним из крупнейших банков Европы и России является российский публичный акционерный банк «Сбербанк России». Он контролируется Центральным банком Российской Федерации и оказывает широкий спектр банковских услуг. С целью обеспечения безопасности информации в ПАО «Сбербанк России» создана система защиты информации, представляющая собой совокупность направлений, требований, средств и мероприятий, сокращающих уязвимость информации и противодействующих незаконному доступу к информации и её утечке.

Для увеличения экономической безопасности ПАО «Сбербанк России» концентрируется на выборе персонала, периодически организовывает инструктажи по безопасности. В контрактах ПАО «Сбербанк России» отчетливо выделены персональные требования, функции к персоналу, а также ответственность за различные нарушения,

так как в большинстве случаев именно он существенно влияет на информационную безопасность банка.

Также, в деятельности Сбербанка широкое распространение получает введение в служебных документах грифа секретности и назначение увеличения суммы оклада для соответствующих категорий персонала.

3.1 Оценка эффективности существующей системы безопасности информации

Настройка политик DLP–системы осуществляется вручную, по результатам обследования бизнес–процессов. По сути, политики представляют собой статичный срез информационной картины бизнеса, склонный к постепенному старению и утрате актуальности.

По опыту внедрения и экспертным оценкам специалистов Сбербанка, совокупную точность (соотношение ложноположительных и ложноотрицательных срабатываний) классической DLP–системы редко удаётся удержать на уровне выше 70%. Дальнейшее повышение точности ведёт к значительному росту затрат на управление и актуализацию политик.

Невысокие показатели точности не позволяют переводить DLP–систему в режим предотвращения утечек (в режим блокировки, «в разрыв») из–за рисков прерывания бизнес–процессов, а служба кибербезопасности сталкивается с целой лавиной ложных срабатываний политик DLP и необходимостью применять разветвлённый набор фильтров для того, чтобы сузить воронку срабатываний до приемлемого уровня. Таким образом, DLP–система, являясь ядром технологического стека процесса защиты от утечек, становится его слабым звеном именно с точки зрения конечного результата: к моменту разбора инцидента по факту утечки сама утечка уже состоялась, а информация покинула периметр.

Радикально поднять точность DLP–систем можно, лишь выполнив два условия:

- принципиально повысить качество политик;
- обеспечить актуальность политик – резко сократить скорость реагирования на изменения, в том числе за счёт пересмотра процесса формирования политик.

Решение этих задач традиционными способами, например, наращиванием вычислительных мощностей или персонала, выглядит неудачной идеей в силу существования принципиально неустранимых проблем ручного труда с его субъективными суждениями, неполнотой и трудностями получения информации.

Для реализации подхода и обучения детектирующих моделей были выбраны типы данных, на которых чаще всего происходят сбои в детекции утечки системой DLP. Массив таких данных был размечен и обогащён набором, который точно относится к анализируемому типу (например, номера паспортов, счетов и т. д.), при этом символьная информация и неструктурированные данные также преобразовываются в цифровой структурированный вид при помощи ещё одних моделей, работающих перед основной. Ансамбль таких моделей помогает

обнаруживать в потоке информации данные счетов, паспортов и банковских карт, при этом для данных, уже преобразованных в цифровой формат, и для ускорения фильтрации применяются регулярные выражения, алгоритмы определения контрольного разряда и Луна.

Ансамбль моделей составляют нейронные сети (в большинстве своём класса NLP– Natural Language Processing) и «классические». Для NLP используются модели CNN и RNN (сверточные и рекуррентные нейронные сети). При обучении использовались различные параметры настройки слоёв нейронных сетей. Не все варианты оказались удачными, но те, что удовлетворяли заданным метрикам по точности, нашли применения в промышленном решении. Модели дополняют друг друга, усиливая точность взаимного результата отнесения анализируемых данных к тому или иному типу и категории защищаемой информации.

Подробнее приведено на врезке 1; на врезке 2 представлены подробные данные по основным типам распознаваемых типов данных. Как мы видим, основной упор делается на поиск персональных данных, так как их охрана – одно из важнейших требований различных регуляторов (законы РФ, ЦБ РФ, GDPR).

Как результат: обучены четыре модели на рекуррентных и сверточных нейросетях на базе NER (Name Entity Recognition). По результатам сравнения качества моделей на валидационной выгрузке отобраны три лучшие из них. Ансамбль из трёх моделей с анализом контрольных разрядов и проверками на регулярных выражениях показывает среднюю точность 95%, из них ~40% атрибутов распознаются с точностью >99,9%.

В первую очередь модели настроены работать с табличными файлами и проходили обучение на структурированных данных, накопленных в аналитическом хранилище данных банка. Также активно разрабатываются модели для работы с текстами и неструктурированной информацией, но это темы для следующих статей. Например, для работы с текстом применяется бэггинг двух CNN–моделей, одной RNN–модели, регулярных выражений и проверок на контрольные разряды. Также проводится исследование качества работы при векторизации, с дальнейшим использованием различных ML–моделей; бэггинг на основе взвешивания фич в векторах.

В банке был успешно проведён пилот по интеграции сервиса распознавания конфиденциальной информации и системы DLP.

Схема реализованного взаимодействия DLP–системы и модели ИИ изображена на рис. 3.1.1.

Рисунок 3.1.1– Схема взаимодействия DLP–системы и модели

При взаимодействии DLP–системы и AI–модели был реализован следующий алгоритм:

- пользователь отправляет сообщение, содержащее подозрительный файл, сообщение перехватывает DLP–система.
- DLP–система направляет уведомление о нарушении программному роботу (специальный модуль, написанный на Python, служащий посредником между моделью и DLP в связи с отсутствием у последней необходимой функциональности).
- программный робот с использованием API–интерфейса забирает подозрительный файл из DLP–системы и передаёт его в исполняемую среду модели.
- модель проводит анализ файла, размечает его и передаёт программному роботу.
- программный робот анализирует размеченный файл и в случае наличия в нём разметки, указывающей на наличие конфиденциальной информации (формат разметки, воспринимаемой роботом, согласовывается заранее), проставляет признак инцидента в карточке события в системе DLP.
- уведомление о подтверждённом инциденте направляется офицеру безопасности (для старта дисциплинарного процесса и т. д.)
- отправителю направляется уведомление о блокировке сообщения в связи с нарушением требований кибербезопасности.
- Измерения показали точность порядка 95–98% на синтетических данных. Предварительная оценка показывает, что при общем количестве событий около 3000 в месяц такая автоматизация

позволит сэкономить не менее 300 человеко–часов, т. е. полноценно заменить трёх квалифицированных офицеров безопасности, причём, в отличие от них, она будет работать в круглосуточном режиме, без перерывов на обед, праздников и выходных.

Конечно, при смене системы DLP приходится заново переписывать реализацию интеграции между системами, поэтому можно либо совершенствовать универсального программного робота, либо сделать программные API для безболезненного перехода с одной системы на другую.

Заключение

ПАО «Сбербанк» играет огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Благодаря своей специфической роли, со времени своего появления они всегда притягивали преступников. К 90–м годам XX века банк перешёл к компьютерной обработке информации, что значительно повысило производительность труда, ускорило расчеты и привело к появлению новых услуг. Однако компьютерные системы, без которых в настоящее время не может обойтись ни один банк, являются также источником совершенно новых угроз, неизвестных ранее. Большинство из них обусловлены новыми информационными технологиями и не являются специфическими исключительно для банков.

Существуют, однако два аспекта, выделяющих банки из круга остальных коммерческих систем:

1. Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д.

2. Она затрагивает интересы большого количества организаций и отдельных лиц.

Поэтому информационная безопасность банка – критически важное условие его существования.

В силу этих обстоятельств, к банковским системам предъявляются повышенные требования относительно безопасности хранения и обработки информации.

Сфера информационной безопасности – наиболее динамичная область развития индустрии безопасности в целом. Если обеспечение физической безопасности имеет давнюю традицию и устоявшиеся подходы, то информационная безопасность постоянно требует новых решений, т.к. компьютерные и телекоммуникационные технологии

постоянно обновляются, на компьютерные системы возлагается все большая ответственность.

Статистика показывает, что подавляющее большинство крупных организаций имеют план с правилами доступа к информации, а также план восстановления после аварий.

Безопасность электронных банковских систем зависит от большого количества факторов, которые необходимо учитывать еще на этапе проектирования этой системы.

При этом для каждого отдельного вида банковских операций и электронных платежей или других способов обмена конфиденциальной информацией существуют свои специфические особенности защиты. Таким образом, организация защиты банковских систем есть целый комплекс мер, которые должны учитывать как общие концепции, но и специфические особенности.

Основной вывод, который можно сделать из анализа развития банковской безопасностии, заключается в том, что автоматизация и компьютеризация банковской деятельности (и денежного обращения в целом) продолжает возрастать. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Можно прогнозировать дальнейшее снижение оборота наличных денег и постепенный переход на безналичные расчеты с использованием пластиковых карт, сети Интернет и удаленных терминалов управления счетом юридических лиц.

Список использованных источников

1. Федеральный закон Российской Федерации от 21.07.1993 № 5485–1 "О государственной тайне" (далее – Закон о государственной тайне).

2. Федеральный закон Российской Федерации Перечень сведений, составляющих государственную тайну, содержится в Указе Президента РФ от 24.01.1998 №61.

3. Федеральный закон Российской Федерации от 27.07.2006 N 149–ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 09.01.2023)

4. Федеральный закон Российской Федерации ст. 12 ФЗ РФ от 15.11.1997г. № 143–ФЗ «Об актах гражданского состояния»

5. Федеральный закон Российской Федерации ст. 243 Трудового кодекса РФ

6. Постановление Правительства РФ от 18 сентября 2006г. № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны»

7. Федеральный закон Российской Федерации № 149 «Об информации, информационных технологиях и о защите информации» от 27.06.2006 г.

8. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 136 с.

9. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. – Рн/Д: Феникс, 2020. – 324 с.

10. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2021. – 384 с.

11. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ–ДАНА, 2018. – 239 с.

12. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ, 2019. – 239 с.

13. Запечников, С.В. Информационная безопасность открытых систем. В 2–х т. Т.1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. – М.: ГЛТ, 2021. – 536 с.

14. Запечников, С.В. Информационная безопасность открытых систем. В 2–х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018. – 558 с. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2022. – 280 с.

15. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2018. – 432 с.

16. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2016. – 296 с.

17. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. – М.: МГИУ, 2017. – 277 с.

18. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2018. – 336 с.

19. Защита информации о https://pandia.ru/text/80/218/40223.phpграниченного доступа |

Организация систем защиты информации с ограниченным доступом – SearchInform

20. Тема 17 п https://pandia.ru/text/80/218/40223.phpравовые основы защиты информации с ограниченным доступом (studfile.net)

21. Статья 9. Огран https://pandia.ru/text/80/218/40223.phpричение доступа к информации \ КонсультантПлюс (consultant.ru)

22. [Электронный ресурс] – Категории инф https://pandia.ru/text/80/218/40223.phpормационных ресурсов по доступу к ним пользователей – Информационное право (studme.org)

23. [Электронный ресурс] – Права доступа https://pandia.ru/text/80/218/40223.phpк ресурсам (studfile.net)

24. [Электронный ресурс] – Информационные р https://pandia.ru/text/80/218/40223.phpесурсы (discovered.com.ua)

25. [Электронный ресурс] – Категории https://pandia.ru/text/80/218/40223.php информационных ресурсов по доступу к ним пользователей – Информационное право (studme.org)

26. [Электронный ресурс] – Информацион https://pandia.ru/text/80/218/40223.phpные ресурсы Банка России и возможности их использования | Контент–платформа Pandia.ru