Содержание:

ВВЕДЕНИЕ

Информационно-коммуникационные технологии (ИКТ), сегодня проникли уже почти в каждую сферу нашей жизни, в том числе, в сферу документооборота. Огромное количество информации циркулирует в электронном виде. Решающую роль в проблеме обеспечения безопасности персональных данных сыграл переход на обработку документов с применением информационных технологий, в частности, с помощью персональных компьютеров и с использованием различных информационных систем (ИС).

ИС является неотъемлемой частью любой современной организации, вне зависимости от ее сферы деятельности и используются повсеместно. Данные системы обслуживают огромное количество клиентов на самых разных уровнях, позволяя автоматизировать работу учреждения в целом. ИС предназначены для обеспечения работоспособности информационной инфраструктуры организации, предоставления различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов организации. Также они позволяют сократить как временные, финансовые, так и трудовые затраты.

Вопрос информационной безопасности (ИБ) ИС стоит на первом месте, ведь в программном обеспечении (ПО) постоянно обнаруживаются уязвимые места и новые ошибки. Сегодня приходится учитывать чрезвычайно широкий спектр программного и аппаратного обеспечения, различные средства инженерно-технической защиты, а также многочисленные связи между компонентами. Защита данных является важнейшей задачей на государственном уровне в любой стране.

Цель настоящей работы – разработка системы защиты банковской системы. В задачи, в соответствии с поставленной целью, входят:

- анализ основных определений и нормативно-правовой базы в области защиты информации и персональных данных (ПДн);
- анализ отделения банка и его деятельности;
- анализ структуры ИС рассматриваемого отделения банка;
- анализ угроз безопасности ИС рассматриваемого отделения банка;

- разработка рекомендаций по защите ИС рассматриваемого отделения банка.

Объектом исследования курсовой работы является система защиты информации (СЗИ) в отделе банка. Предметом исследования является организация безопасности информации и ПДн, циркулирующей в ИС данного учреждения.

Безопасность информации в организации

Нормативная база в области защиты информации

ПДн всех субъектов нуждаются в защите. Эти и другие возможные обстоятельства подтверждают необходимость правового закрепления методов, относительно обработки ПДн, правил их хранения и использования в организации, о передаче ПДн третьим лицам, а также об ответственности граждан за несоблюдение правовых норм, регулирующих указанные вопросы. Институт ПДн - часть новой для РФ правовой системы ветви - информационного права. Законодательное оформление информационного права в отдельную ветвь берет своё начало в 80-х гг. XX столетия, ввиду бурного развития ИТ.

Согласно Российской Конституции [1] ПДн относятся к группе конфиденциальной информации, и предполагается, что сбор, хранение и распространение информации о частной жизни лица без его одобрения запрещён (ст. 24 гл. 2 Конституции РФ).

Конфиденциальная информация – это коммерческая, военная, банковская, служебная или государственная тайна [2]. Как правило, конфиденциальная информация может представлять собой особую категорию и относиться к коммерческой тайне. Ниже представлен состав конфиденциальных документов.

1. нормативно-методические;
2. руководящие;
3. распорядительные;
4. информационно-справочные;
5. организационные;
6. финансово-бухгалтерские;
7. кадровые (по личному составу).

Все виды сведений, сохранность которых защищается на законодательном уровне, перечислены в одноименном перечне, утвержденном Указом Президента России от 06.03.1997 № 188. Так, в соответствии с документом, к категории конфиденциальной информации относятся:

1. ПДн гражданина;
2. сведения, составляющие служебную тайну;
3. профессиональная тайна;
4. коммерческая тайна;
5. содержание личных дел осужденных за совершение преступлений;
6. информация об исполнении судебных решений в рамках исполнительного производства;
7. информация, составляющая тайну судопроизводства и следствия, в том числе данные о свидетелях и потерпевших, подлежащих государственной защите, а также о судьях и должностных лицах следственных и правоохранительных органов.

Возникновение и развитие института Персональных данных напрямую связано с историей становления прав и свобод человека, в особенности с правом на неприкосновенность личной жизни. В РФ нормативной основой для защиты Персональных данных является Федеральный закон «О персональных данных» № 152-ФЗ от 17.07.2006 [3]. Данный ФЗ является основополагающим законом в области регулирования вопроса, связанного с обработкой ПДн, и определяет:

1. основные понятия, связанные с обработкой ПДн;
2. принципы и условия обработки ПДн;
3. обязанности оператора ПДн;
4. права субъекта ПДн;
5. виды ответственности за нарушение требований закона № 152-ФЗ;
6. государственные органы, осуществляющие контроль над соблюдением требований закона № 152-ФЗ.

Требования закона № 152-ФЗ распространяются при обработке ПДн, как федеральными органами государственной власти, так и органами государственной власти субъектов РФ, органами местного самоуправления, муниципальными органами, юридическими и физическими лицами.

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту

персональных данных).

Персональные данные разделяют на следующие категории: общедоступные, специальные, биометрические и иные (Таблица 1).

Таблица 1

Категории персональных данных

Категория	**Виды данных**
общедоступные ПДн	1. данные, доступ к которым разрешен субъектом персональных данных; 2. данные, на которые не распространяется требование конфиденциальности в соответствии с ФЗ
специальные ПДн	1. сведения о расовой или национальной принадлежности; 2. данные, касающиеся политических, религиозных или философских убеждений; 3. информация о состоянии здоровья, об интимной жизни.
биометрические ПДн	1. сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность
иные ПДн	1. все, что не попало ни в одну из вышеуказанных категорий

В качестве операторов ПДн могут выступать государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее обработку ПДн.

Обработка ПДн заключается в совершении ряда операций по сбору, записи, систематизации, накоплению и т.д. Причем осуществляться действия могут как с использованием средств автоматизации, так и без их применения.

В таблице 2 продемонстрирован перечень возможных деструктивных действий по отношению к ПДн.

Таблица 2

Обработка ПДн

Действие	Описание
Распространение	Раскрытие ПДн неопределенному кругу лиц
Предоставление	Раскрытие ПДн определенному кругу лиц
Блокирование	Временное прекращение обработки ПДн
Уничтожение	Результатом данного процесса становится невозможность восстановления ПДн или уничтожение материальных носителей
Обезличивание	В результате данных действий становится невозможным определить владельца ПДн без использования дополнительной информации
Трансграничная передача	Передача ПДн на территорию другого государства

Оператор ПДн обрабатывает информацию с согласия субъекта ПДн. Согласие должно быть конкретным, информированным и сознательным.

В соответствии с нормативными документами в области защиты информации, каждое предприятие и организация, в которой производится обработка персональных данных, обязано принять ряд организационных и технологических мер по обеспечению защиты информации. Ниже представлена часть нормативных документов, которые касаются обработки ПДн и обеспечения их безопасности:

1. Федеральный закон РФ от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации» [4];
2. Федеральный закон РФ от 27.07.2006 № 152 «О персональных данных»;

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - ПП «Об утверждении требований к защите ПДн при их обработке в ИСПДн») [5];
4. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных».
5. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [6];
6. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн, утвержденная 15.02.2008 г. ФСТЭК России;
7. Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденная ФСТЭК России;
8. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации, утвержденная ФСБ России;
9. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности № 149/7/2/6-432 от 31 марта 2015 года.

Основой этих всех документов является концепция защиты средств вычислительной техники и ИСПДн от НСД к информации и основные принципы защиты компьютерных систем.

В имеющих сейчас базовое значение документах, регулирующих работу с ПДн в РФ, сформулированы основные принципы работы с ПДн:

1. ПДн должны собираться и обрабатываться (храниться, использоваться, раскрываться, стираться и т.д.) только в соответствии с законом и наделенными соответствующими полномочиями органами;
2. ПДн должны быть адекватными заранее определенным целям и распоряжение ими должно ограничиваться по срокам, соответствующим указанным целям;
3. ПДн должны быть точны;
4. ПДн должны обрабатываться с согласия субъектов этих данных;

5. ПДн должны быть доступны субъектам этих данных, в том числе и для внесения уточнения в эти данные;
6. ПДн должны быть должным образом защищены.

Угрозы безопасности и уязвимости ИСПДн организации

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы (АИС), которые могут быть использованы для реализации угрозы безопасности ПДн.

Причинами возникновения уязвимостей являются:

1. ошибки при проектировании и разработке ПО;
2. преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки ПО;
3. неправильные настройки ПО, неправомерное изменение режимов работы устройств и программ;
4. несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов;
5. внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
6. несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
7. сбои в работе ПО и аппаратуры (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и др.).

Ниже представлена общая характеристика основных групп уязвимостей ИСПДн, включающих:

1. уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
2. уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

При определении актуальных угроз безопасности организации, в первую очередь, необходимо рассмотреть угрозы ИС.

Требования по обеспечению безопасности ПДн в организации

Требования по защите ПДн в организации подразумевают под собой комплекс средств и методов, обеспечивающих конфиденциальность и сохранность ПДн. В зависимости от требуемого уровня защищённости (или защиты) ПДн предъявляются разные требования по обеспечению их безопасности: чем выше требуемый уровень защищённости ПДн, тем шире перечень необходимых мер. Соответственно, прежде чем определить состав и содержание технических и организационных мер по защите ПДн, необходимо определить уровень защищённости ПДн.

Требуемый уровень защищённости ПДн при их обработке в ИСПДн зависит от:

1) типа угроз, актуальных для ИСПДн,

2) категории обрабатываемых ПДн.

Тип актуальных угроз определяется в соответствии с п. 6 ПП № 1119.

Если ПДн обрабатываются с использованием информационных систем, то необходимо определить уровень защищенности ПДн, опираясь на Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн» (таблица 3) [7].

От уровня защищенности ПДн в ИСПДн зависит объем мероприятий по их защите и выбор систем защиты. Определение минимального класса СКЗИ представлено в таблице 4 и определяется Приказом ФСБ РФ от 10.07.2014 № 378 .

Таблица 3

Определение уровня защищенности ПДн

Тип ИСПДн	**Категории субъектов**	**Количество субъектов**	**Тип актуальных угроз**		
			1 тин (ВДВ в СПО)	**2 тип (НДВ в НПО)**	**3 тип (нет НДВ)**

		Более 100 000	УЗ 1	УЗ 1	УЗ 2
Специальные	11с сотрудников	Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Любое	УЗ 1	УЗ 2	УЗ 3
Биометрические	Любых	Любое	УЗ 1	УЗ 2	УЗ 3
		Более 100 000	УЗ 1	УЗ 2	УЗ 3
Иные	11е сотрудников	Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 1	УЗ 3	УЗ 4
		Более 100 000	УЗ 2	УЗ 2	УЗ 4
Общедоступные	11е сотрудников	Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Любое	УЗ 2	УЗ 3	УЗ 4

Таблица 4

Определение минимального класса СКЗИ

Уровень защищенности ПДн	4	УЗ 3	УЗ	2	УЗ		1	УЗ	
Тип актуальных угроз	3	2	3	1	2	3	1	2	

Минимальный класс СКЗИ КС1 КВ КС1 КЛ КВ КС1 КЛ КВ

Определение минимального перечня мероприятий по ЗИ (Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн») представлено в таблице 5.

Таблица 5

Определение минимального перечня мероприятий по ЗИ

Перечень мер защиты	1 2 3 4 У У У У З З З З
Организовать режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц. нс имеющих прав доступа в эти помещения	+ + + +
Обеспечить сохранность носителей ПДн	+ + + +
Утвердить перечень лиц, имеющих доступ к ПДн в рамках выполнения своих служебных обязанностей	+ + + +
Использовать сертифицированные СЗИ	+ + + +
Назначить приказом должностное лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.	+ + +

Доступ к электронному журналу сообщений определить только лицам, которым необходимы сведения, содержащиеся в данном журнале для выполнения своих служебных обязанностей	+ +
Обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочии сотрудника по доступу к ПДн в ИСПДн	+
Создать структурное подразделение ответственное за обеспечение безопасности ПДн в ИСПДн или возложить эти функции по обеспечению безопасности ПДн в ИСПДн на одно из существующих структурных подразделении	+

Выводы

Первая глава курсовой работы посвящена теоретическому анализу нормативно-правовых актов, действующих в сфере защиты ПДн, а также анализу угроз и уязвимостей, которым подвержена ИСПДн организации. Были описаны требования по защите информации ПДн в организации.

Анализ объекта защиты и рекомендации по защите информации в банковской системе

Инфраструктура отделения банка

Защищаемое отделение банка начало свою деятельность в 2011 г. Подразделение занимается оформлением кредитов, расчетно-кассовыми операциями, также осуществляет ряд функций ПФР, в частности, по выплате пособий и пенсий. В банке можно осуществить оплату коммунальных услуг и погасить штрафы. Банк плотно сотрудничает с государственными учреждениями, аккредитован и работает с самыми различными видами конфиденциальной информации - персональными данными клиентов, коммерческими сведениями юридических лиц и другими данными.

Численность сотрудников отделения составляет 20 человек, функциональные обязанности которых распределены в соответствии с должностными инструкциями. Архитектура сети (точнее топология) банка представлена по типу «Звезда», что имеет значительное влияние на ее отказоустойчивость и управляемость.

ИС рассматриваемого отдела банка позволяет автоматизировать работу сотрудников банка. В рамках разработки ИС была автоматизирована следующая информационно-аналитическая деятельность бизнес-процессов:

- ведение базы договоров с клиентами банка по финансовым вопросам (кредиты, займы, вклады и т.п);
- ведение базы ПФР;
- осуществление субсидирования контрагентов банка;
- составление итоговых отчетов о деятельности подразделения.

Данные процессы подразумевают циркуляцию персональных и конфиденциальных данных клиентов внутри банка между автоматизированными рабочими местами (АРМ) сотрудников (рисунок 1).

Рисунок 1. Циркуляция информации в системе банка

К основным функциям ИС банка следует отнести:

1. Автоматизацию всех ежедневных внутрибанковских операций, ведение бухгалтерии и составление сводных отчетов.
2. Системы коммуникаций с филиалами и иногородними отделениями.
3. Системы автоматизированного взаимодействия с клиентами (так называемые системы «банк-клиент»).
4. Аналитические системы. Анализ всей деятельности банка и системы выбора оптимальных в данной ситуации решений.

5. Автоматизацию розничных операций - применение банкоматов и кредитных карточек.
6. Системы межбанковских расчетов.
7. Системы автоматизации работы банка на рынке ценных бумаг.

ИС имеет трехуровневую архитектуру (АРМ менеджера – сервер приложений - сервер базы данных), которую можно разделить на три уровня (рисунок 2).

Рисунок 2. Структура банковской системы

В ИС присутствуют и другие функциональные подсистемы:

- хранения данных;
- возможности операционного управления;
- управление настройками ИС;
- создания отчетов.

Общий вид ИС изображен на схеме ниже (рисунок 3).

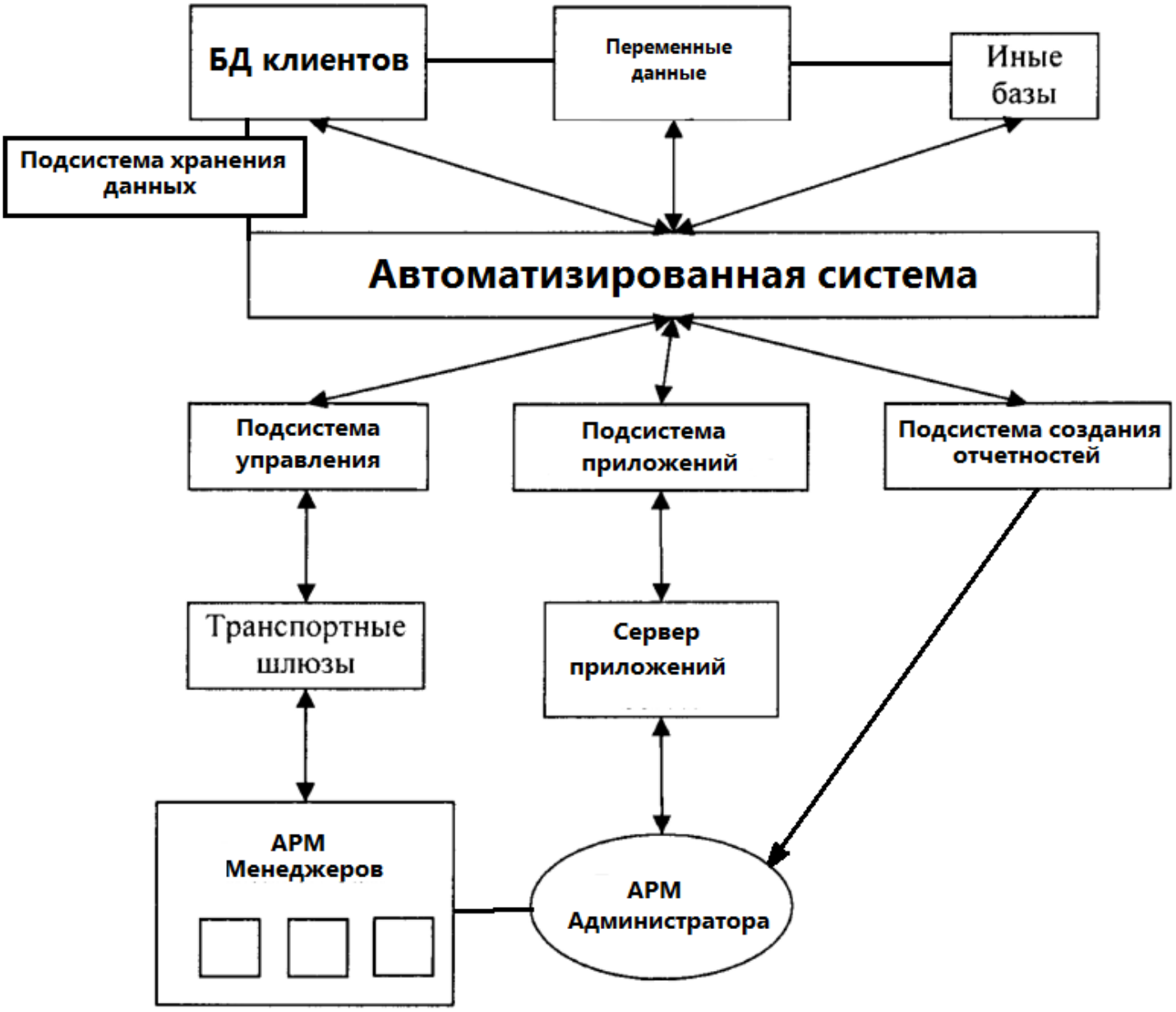


Рисунок 3. Схема банковской системы

Подсистема хранения данных (предназначена для хранения данных в структурах, нацеленных на обеспечение процесса принятия решений).

Подсистема приложений операционного управления **(**предназначена для взаимодействия компонентов системы, вывода информации о клиентах).

Подсистема управления настройками ИС **(**предназначена для ведения справочников настроек, используемых для обеспечения информационной совместимости компонентов системы).

Подсистема создания отчетности **(**предназначена для создания форм регламентированной отчетности, настройки параметров и видов отчетов в различных форматах).

Смежными системами для ИС являются следующие подсистемы, развернутые на АРМ:

- ИС оперативной обработки данных Заказчика (1С Бухгалтерия 8);
- ИС планирования (1С Бухгалтерия 7).

Источниками данных для ИС являются:

- ИС управления предприятием (СУБД MS SQL).
- Информационно-справочная система (СУБД MS SQL).
- ИС обеспечения бюджетного процесса (СУБД Oracle).

Перечень предпочтительных способов взаимодействия со смежными системами приведен ниже:

- ИС управления предприятием - с использованием промежуточной базы данных (ПБД).
- Информационно-справочная система - обмен файлами ОС определенного формата.
- ИС обеспечения бюджетного процесса - интеграция по принципу «точка – точка».

Системное ПО отделения банка ВТБ основано на:

- ОС Windows 10 на ПК, наличие которых позволяет работать с возможностями Active Directory, а также другими возможностями.
- серверной ОС Windows 2016 Server, в работе которой используются возможности контроля учетных записей пользователей средствами Active Directory.

Серверное ПО отделения банка ВТБ содержит:

- контроллер домена;
- сервер управления доступом в Интернет, с использованием которого производится установка прав доступа на пользование внешними сетями, установка лимитов, ограничений доступа к определенным сайтам, учет трафика;

- систему управления электропитанием.

Прикладное ПО:

- бухгалтерия работает с 1С: Предприятие 8.3, Сбербанк Бизнес Онлайн», Гарант, Налогоплательщик ЮЛ, Spu orb. Консультант +, Гарант; а также специализированные программные продукты.

С использованием средств автоматизации ПДн обрабатываются в информационной системе персональных данных (ИСПДн) и системе персонифицированного учета (СПУ).

ИСПДн СПУ является информационной системой федерального масштаба с расположением ключевых узлов во всех регионах РФ.

Структурная схема ИСПДн СПУ представлена на рисунке 4.

Рисунок 4. Структурная схема ИСПДн банка

Угрозы безопасности банковской системы

Угроза ИБ персональных данных реализуется в результате образования канала реализации между источником угрозы и объектом воздействия, что создает необходимые условия для нарушения ее безопасности.

Каналы реализации угрозы по своей составляющей могут быть [8]:

- физическими угрозами (непосредственный доступ к ИС);
- сетевыми угрозами (удаленный доступ к ИС);
- программными угрозами (доступ к ИС из программной среды);
- аппаратными (доступ к ИС из аппаратной среды).

Основными элементами процесса описания угроз утечек информации по техническим каналам являются: источник реализации угрозы, канал распространения информативного сигнала, а также информационный актив на который воздействует нарушитель.

В ИСПДн рассматриваемого банка возможны:

1. Угрозы, реализуемые в ходе загрузки ОС:

- перехват паролей или идентификаторов;
- модификация базовой системы ввода/ вывода (BIOS), перехват управления загрузкой;

2. Угрозы, реализуемые после загрузки ОС:

- выполнение несанкционированного доступа (НСД) с применением стандартных функций ОС;
- выполнение НСД с помощью прикладной программы (например, системы управления базами данных (СУБД);
- выполнение НСД с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т.п.);
- утечка информации с использованием копирования ее на съемные, носители;
- утечка информации за счет ее несанкционированной передачи по каналам связи;

3. Угрозы внедрения вредоносных программ с использованием съемных носителей;

4. Угрозы утечки информации с помощью аппаратных закладок;

5. Угрозы «Анализа сетевого трафика» - перехват передаваемой во внешние сети и принимаемой из внешних сетей информации;

6. Угрозы сканирования - выявление типа или типов, используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

7. Угрозы получения НСД путем подмены доверенного объекта:

- обход системы идентификации и аутентификации сообщений;
- обход системы идентификации и аутентификации сетевых объектов.

8. Угрозы внедрения ложного объекта сети - перехват запросов и модификация адресных данных (с использованием протоколов SAP, ARP, DNS, WINS).

9. Угрозы навязывания ложного маршрута - несанкционированное изменение маршрутно-адресных данных (с использованием протоколов RIP, OSPF, LSP, ICMP, SNMP)

10. Угрозы выявления паролей:

11. Угрозы типа «Отказ в обслуживании»;

12. Угрозы удаленного запуска приложений:

- внедрение троянских программ;
- атаки типа «переполнение буфера»;
- с использованием средств удаленного управления;

13. Угрозы внедрения по сети вредоносных программ:

- внедрение вредоносных программ через почтовые сообщения;
- внедрение вредоносных программ через обмен и загрузку файлов;
- внедрение вредоносных программ через зараженные веб-страницы;

Обеспечение безопасности банковской системы

Определение класса защищенности ИСПДн банка

Классификация ИСПДн необходима для надлежащего определения мер, необходимых для достижения требуемого уровня информационной защиты. Для определения актуальных угроз ИСПДн была определена исходная степень защищенности ИСПДн (таблица 6).

Таблица 6

Исходная степень защищенности ИСПДн организации

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	Средний	Низкий
1. По территориальному размещению.	0	0	1

2. По наличию соединения с сетями общего пользования.	0	0	1
3. По встроенным (легальным) операциям с записями баз ПДн.	0	1	0
4. По разграничению доступа к ПДн	0	1	0
5. По наличию соединений с другими базами ПДн иных ИСПДн.	1	0	0
6. По уровню обобщения (обезличивания) ПДн.	0	1	0
7. По объему ПДн, которые предоставляются сторонним пользователям.	1		0

В соответствии с Таблицей 6, менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», следовательно, Y1=5, а ИСПДн организации имеет среднюю степень исходной защищенности.

Определение вероятности и возможности реализации УБПДн осуществляется экспертным методом. При определении актуальности угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

0 – для маловероятной угрозы (отсутствуют объективные предпосылки для осуществления угрозы);

2 – для низкой вероятности угрозы (объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию);

5 – для средней вероятности угрозы (объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны);

10 – для высокой вероятности угрозы (объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты).

Была проведена оценка вероятности реализации УБПДн различными категориями нарушителей (таблица 7).

Таблица 7

Оценка вероятности реализации УБПДн различными категориями нарушителей

№	Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем						Итого Y2
		B1	B2	B3	K1	K2	K3	
1	Угроза перехват паролей или идентификаторов	5	5	2	0	0	0	5
2	Угроза модификации базовой системы ввода/ вывода, перехват управления загрузкой	0	0	0	0	2	0	0
3	Угроза выполнения НСД с применением стандартных функций операционной системы	10	10	2	0	5	5	10
4	Угроза выполнения НСД с помощью прикладной программы	10	10	0	0	5	5	10
5	Угроза выполнения НСД с применением специально созданных для выполнения НСД программ	5	5	0	0	0	0	5
6	Угроза утечки информации с использованием копирования ее на съемные, носители	0	0	0	2	5	2	2

7	Угроза утечки информации за счет ее передачи по каналам связи	10	10	0	0	2	2	10
8	Угроза внедрения вредоносных программ с использованием съемных носителей	2	2	2	2	5	5	5
9	Угроза утечки информации с помощью аппаратных закладок	0	0	0	0	0	0	0

В – внешний нарушитель. Действия внешнего нарушителя носят намеренный и деструктивный характер.

$В_1$ - криминальные структуры (организованные группировки, хакеры);

$В_2$ - конкуренты (недобросовестные партнеры, конкурирующие структуры);

$В_3$ – инсайдеры (физические лица, бывшие работники компании).

В таблице 8 приводится описание внутренних нарушителей.

Таблица 8

Описание внутренних нарушителей

№	Тип внутреннего нарушителя	Возможности
К1	Обслуживающий персонал	Повреждение линий связи и элементов ЛВС
К2	Локальные пользователи	Ошибки в системном и прикладном программном обеспечении, нарушение конфиденциальности

К3	Удаленные пользователи	Ошибки в системном и прикладном программном обеспечении, нарушение конфиденциальности и доступности

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y), а также определяется возможность реализации угрозы и опасность угрозы.

Коэффициент реализуемости угрозы Y определялся соотношением:

Y=(Y1+Y2)/20

при этом каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

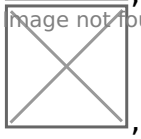
10 – для низкой степени исходной защищенности.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если 

, то возможность реализации угрозы признается низкой;
- если 

, то возможность реализации угрозы признается средней;
- если 

, то возможность реализации угрозы признается высокой;
- если 

, то возможность реализации угрозы признается очень высокой.

Опасность угрозы оценивается с привлечением компетентного специалиста в области ИБ, значения опасности определяются в соответствии со следующими заключениями:

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

Параметры вероятности реализации, возможности реализации и опасности угроз приведены в таблице 9.

Таблица 9

Параметры вероятности реализации, возможности реализации и опасности угроз организации

№	Угроза безопасности ПДн	Коэффициент реализуемости угрозы Y	Возможность реализации угрозы	Опасность угрозы
1	Угроза перехват паролей или идентификаторов	0,5	Средняя	Средняя
2	Угроза модификации базовой системы ввода/ вывода, перехват управления загрузкой	0,25	Низкая	Низкая
3	Угроза выполнения НСД с применением стандартных функций операционной системы	0,75	Высокая	Средняя

4	Угроза выполнения НСД с помощью прикладной программы	0,75	Высокая	Средняя
5	Угроза выполнения НСД с применением специально созданных для выполнения НСД программ	0,5	Средняя	Высокая
6	Угроза утечки информации с использованием копирования ее на съемные, носители	0,35	Средняя	Средняя
7	Угроза утечки информации за счет ее несанкционированной передачи по каналам связи	0,75	Высокая	Средняя
8	Угроза внедрения вредоносных программ с использованием съемных носителей	0,5	Средняя	Высокая
9	Угроза утечки информации с помощью аппаратных закладок	0,25	Низкая	Низкая

Актуальность угроз определяется на основании данных из таблицы 9 и методики выбора актуальных угроз из таблицы 10.

Таблица 10

Методика выбора актуальных угроз

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Перечень угроз безопасности ИСПДн и приведен в таблице 11.

Таблица 11

Актуальные угрозы организации

№	**Угроза безопасности ПДн**	**Актуальность угрозы**
1	Угроза перехват паролей или идентификаторов	Актуальная
2	Угроза модификации базовой системы ввода/ вывода, перехват управления загрузкой	Неактуальная
3	Угроза выполнения несанкционированного доступа с применением стандартных функций операционной системы	Актуальная
4	Угроза выполнения несанкционированного доступа с помощью прикладной программы	Актуальная

5	Угроза выполнения несанкционированного доступа с применением специально созданных для выполнения НСД программ	Актуальная
6	Угроза утечки информации с использованием копирования ее на съемные, носители	Актуальная
7	Угроза утечки информации за счет ее несанкционированной передачи по каналам связи	Актуальная
8	Угроза внедрения вредоносных программ с использованием съемных носителей	Актуальная
9	Угроза утечки с помощью аппаратных закладок	Неактуальная

Утвержденная ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработана ФСТЭК России на основании закона № 152-ФЗ, предназначена для использования при проведении работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

ИСПДн присвоен региональный масштаб. Также согласно типу обрабатываемой информации в ИС отдела банка, а также документу «Акт классификации АС, предназначенной для обработки конфиденциальной информации», учитывая условия эксплуатации системы, и в соответствии с руководящими документами Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», рассматриваемой информационной системе присвоен 2-ой класс защищенности. Данная система классифицирована, как многопользовательская АС, в которой одновременно происходит обработка и хранение информации различных уровней конфиденциальности.

Рекомендации по защите банковской системы

Основные направления использования программной защиты информации ИС от НСД заключаются в защите [9]:

- программ от копирования,
- информации от разрушения,
- информации от вирусов,
- программ от вирусов.

Также для защиты от несанкционированного вторжения предпринимаются определенные меры безопасности. Особые функции, которые должны осуществляться программными средствами, это:

- идентификация объектов и субъектов;
- разграничение доступа к вычислительной технике;
- контроль и регистрация действий с информацией и программами.

В процедурах идентификации используются различные методы:

- простые, сложные и одноразовые пароли;
- обмен вопросами и ответами с администратором;
- средства анализа индивидуальных характеристик,

После идентификации защита осуществляется на 3 уровнях:

- аппаратуры;
- ПО;
- данных ИС.

Также для защиты информации в ИС компании позволит организация разграничения доступа через настройку системы защиты, ведение системы логических имен и личных кодов пользователей ИС, установка специальных программных средств контроля доступа к информационным ресурсам, использование криптографических методов защиты, соблюдение правил данной инструкции в части работы пользователей ИС. Все описанные процедуры необходимо отразить в соответствующих нормативных документах банка.

Ключевой же мерой противодействия угрозам информационной безопасности ИСПДн является создание и внедрение системы защиты персональных данных (СЗПДн).

СЗПДн представляет собой системный комплекс решений, направленный на нейтрализацию, противодействие и минимизацию угроз ИБ и состоящий из следующих мероприятий:

- технические мероприятия;
- организационные мероприятия.

Технические мероприятия состоят из инсталляции и настройки средств защиты информации:

- средство защиты от НСД;
- средство антивирусной защиты;
- средство межсетевого экранирования и защиты каналов связи.

Средство защиты от НСД предназначено для:

- разграничения доступа пользователей к информационным ресурсам;
- аудита пользовательских действий;
- контроля активности съемных носителей;
- контроля целостности программной среды (файлов, каталогов, объектов системного реестра);
- сообщения о изменении в программных компонентах;

Средство антивирусной защиты предназначено для:

- недопущения попадания вредоносного ПО на средства вычислительной техники ИСПДн;
- противодействию активного заражения;

Средство межсетевого экранирования и защиты каналов связи предназначено для [10]:

- фильтрации входящего и исходящего трафика;
- защиты сетевого трафика в каналах связи, передаваемого через сети связи общего доступа;

Организационные мероприятия предназначены для создания регламентационной базы по эксплуатации средств защиты информации и состоят из следующих мероприятий:

- назначение ответственных лиц за эксплуатацию СЗПДн и регламентацию их деятельности;
- обучение пользователей правилам ИБ при работе в ИСПДн;
- периодический пересмотр и актуализацию модели угроз.

Заключительным этапом при построении системы защиты, является аттестация данной системы. Аттестация объекта - комплекс мероприятий, в результате которых посредством «Аттестата соответствия» подтверждается, что данный объект соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК, ФСБ России или другими органами государственного управления в пределах их компетенции. Аттестат соответствия требуется для получения лицензии, например, по осуществлению деятельности, связанной с разработкой системы защиты информации или деятельности по технической защите конфиденциальной информации. Для всего этого необходим Аттестат соответствия автоматизированной системы и защиты помещения, который соответствует требованиям по ИБ.

При осуществлении работ по защите конфиденциальной информации также необходимо проведение аттестационных мероприятий. Данное положение определенно федеральным законом № 152 от 27.07.2006.

Аттестация выполняется в несколько этапов, каждый из которых влечет за собой некоторые дополнительные работы, связанные со спецификой аттестуемых объектов: начиная от определения местоположения, технических характеристик объекта, и заканчивая проведением специальных исследований.

В рамках Аттестации объектов информатизации (ОИ) выдвигаются требования, предъявляемые законодательством, а именно, следующими документами:

- Руководящим документом ФСТЭК России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- Нормативно-методическим документом «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

Исходя из Руководящего Документа, требования для ОИ выдвигаются после определения его класса защищенности. Именно данные требования можно использовать для оценки соответствия ОИ требованиям по защите информации от

НСД. Система сопровождения процесса аттестации устроена таким образом, что после определения класса защищенности она выдвигает требования к следующим подсистемам:

- управление доступом (идентификация, аутентификация);
- регистрация событий;
- шифрование информации;
- контроль целостности (как отдельных программ, так и самих СЗИ).

Для аттестации ИСПДн помимо тех требований, которые сформулированы в СТР-К, могут выдвигаться дополнительные требования для конкретного уровня защищенности, а также меры по их реализации. Требования выдвигаются для актуальных угроз, определенных базовой моделью угроз.

Аттестацию ОИ осуществляют лицензиаты ФСТЭК и ФСБ на основе распорядительных документов, правовых норм и прочих регламентов.

Выводы

В данной главе была проанализирована ИСПДн рассматриваемого отделения банка. Были описаны актуальные угрозы банковской системы, определен класс защищенности данной системы.

На основании проведённого анализа, были даны рекомендации по защите банковской системы рассматриваемого отделения банка.

ЗАКЛЮЧЕНИЕ

Информационная безопасность данных, вне зависимости от того, какой характер они носят и каким образом циркулируют – ключевая задача в любой современной организации, тем более, связанной по деятельности с конфиденциальными сведениями, примером чего является отдел банка. Данная задача носит комплексный характер и требует всестороннего подхода, в частности, в области защиты ИСПДн банка.

В ходе выполнения курсовой работы были решены следующие задачи:

- проанализирована нормативная база в области защиты информации
- проанализирована структура банковской системы объекта защиты.

- проанализированы угрозы безопасности банковской системы.
- разработаны рекомендации по улучшению защиты информации, циркулирующей в ИСПДн отделения банка.

В ходе выполнения данной работы были приобретены знания и практические навыки, которые будут полезны будущем. Цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Конституция РФ : [принята всенар. Голосованием 12 декабря 1993 г.] : офиц. текст : по сост. на 21 июля 2014 г. – М. : Инфра-М
2. Гостехкомиссия России. «Руководящий документ: Защита от НСД к информации. Термины и определения», - Москва, 1992. // Доступ из справочно-правовой системы «КонсультантПлюс». 15.10.2019.
3. Федеральный закон «О персональных данных» № 152-ФЗ от 17.07.2006;
4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
5. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн» (далее - ПП «Об утверждении требований к защите ПДн при их обработке в ИСПДн»);
6. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПдн» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) // Доступ из сайта ФСТЭК. 15.10.2019.
7. Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в ИСПДн»
8. Руководящий документ «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требований по защите информации». Государственная техническая комиссия при Президенте РФ (Гостехкомиссия России).
9. Асокин В.В. Основы информационной безопасности / В.В. Асокин. – М.: КУБГУ, 2012. – 297 с.
10. Основы информационных технологий: учебное пособие / Г.И. Киреева, В.Д. Курушин, А.Б. Мосягин, Д.Ю. Нечаев, Ю.В. Чекмарев. – Саратов: Профобразование, 2017. – 272 с.