Инфосистемы Джет

УТВЕРЖДАЮ

и.о. Председателя Правления
ОАО «Челябинвестбанк»

_____ С.М. Бурцев

«_____» _____ 2011 г.

УТВЕРЖДАЮ

Заместитель Генерального директора
по финансовому и оперативному
управлению ЗАО «Инфосистемы Джет»

_____ А.М. Козлов

«_____» _____ 2011 г.

ОАО «Челябинвестбанк»

Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ИСПДн

СОГЛАСОВАНО

Заместитель Председателя Правления
ОАО «Челябинвестбанк»,
начальник управления автоматизации

_____ И.С. Юдович

«_____» _____ 2011 г.

СОГЛАСОВАНО

Начальник
Центра информационной безопасности
ЗАО «Инфосистемы Джет»

_____ И.В. Ляпунов

«_____» _____ 2011 г.

Москва
2010

Определения и сокращения

ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
СЗПДн	Система защиты персональных данных
Блокирование персональных данных	Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи
Информационная система персональных данных	Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
Использование персональных данных	Действия (операции) с персональными данными, совершаемые Банком в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц
Конфиденциальность персональных данных	Обязательное для соблюдения Банком или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания
Обезличивание персональных данных	Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных
Обработка персональных данных	Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных
Общедоступные персональные данные	Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности
Персональные данные	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
Распространение персональных данных	Действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом
Трансграничная передача персональных данных	Передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства
Уничтожение персональных данных	Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных
Уполномоченное лицо Банка	Представитель Банка, являющийся подразделением, работником Банка или сторонней организацией, действующей на основании Договора, заключенного между Банком и этой организацией в рамках действующего законодательства РФ, ответственные за обеспечение безопасности ПДн

1 Общие положения

1.1 Назначение документа

1.1.1. Настоящее Положение определяет состав персональных данных в ОАО «Челябинвестбанк» (далее – Банк), цели и способы обработки персональных данных, порядок обработки персональных данных работников Банка и иных субъектов персональных данных, устанавливает ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2 Правовые и нормативно-методические источники документа

1.2.1. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми документами:

- Статья 24 Конституции Российской Федерации;
- Глава 14 Трудового Кодекса Российской Федерации;
- Федеральный закон Российской Федерации №152-ФЗ «О персональных данных» от 27.07.2006 г.;
- Федеральный закон № 149-ФЗ «об информации, информационных технологиях и о защите информации» от 27.07.2006 г.;
- Постановление Правительства Российской Федерации «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» № 781 от 17 ноября 2007 г.;
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- Методические рекомендации ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных

системах персональных данных» (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.);

- Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное Приказом ФСТЭК России от 5 февраля 2010 г. № 58;
- Политика обеспечения безопасности информации в автоматизированной системе ОАО «Челябинвестбанк».

1.3 Область действия документа

1.3.1. Положения настоящего документа обязательны для исполнения всеми работниками Банка, контрагентами и третьими сторонами, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования по защите персональных данных.

1.3.2. Действие настоящего документа распространяется на все информационные системы персональных данных Банка.

1.4 Порядок ввода в действие и изменение Положения

1.4.1. Настоящее Положение вступает в силу с момента его утверждения Председателем Правления Банка.

1.4.2. Все изменения в Положение вносятся приказом.

2 Цели и правовое основание обработки персональных данных

2.1. Обработка персональных данных работников Банка осуществляется в целях, регулирования трудовых отношений между Банком и работниками, содействия работникам в выполнении ими своих функциональных обязанностей, обучении, продвижении по работе, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Банка, очередности предоставления отпусков, установления и расчета размера заработной платы, страхования работников, оформления страховых свидетельств государственного пенсионного страхования, обеспечения пропускного режима Банка, учета времени, проведенного работником в помещении Банка, а также в иных целях, необходимых Банку в связи с трудовыми отношениями с работниками Банка.

2.2. Обработка персональных данных субъектов персональных данных, не являющихся работниками Банка, осуществляется в целях обеспечения выполнения работ и предоставления услуг, определенных Уставом и лицензиями Банка, выполнения договорных обязательств Банка перед клиентами, предоставления возможности работникам контрагентов Банка выполнения обязанностей, предусмотренных договорами между Банком и его контрагентами.

3 Информационные системы персональных данных

Состав, категории и местонахождение ПДн определяют замысел защиты при обработке ПДн в ИСПДн Банка.

3.1 Состав и местонахождение ПДн

3.1.1. В Банке обрабатываются персональные данные следующих субъектов ПДн:

- работники Банка;
- иные субъекты ПДн – клиенты (контрагенты) Банка.

3.1.2. Персональные данные работников Банка содержатся в документах персонального учета работников – личном деле, трудовой книжке, выдаваемых доверенностях (при наличии), а также в иных документах, формируемых в процессе осуществления профессиональной деятельности Отдела по работе с персоналом, Департамент бухгалтерского учета и отчетности Банка. Персональные данные работников содержатся также в информационных системах Банка, доступ к которым предоставлен ограниченному кругу работников Банка.

3.1.3. ПДн клиентов (контрагентов) Банка содержатся в заключаемых с ними договорах, документах, относящихся к исполнению данных договоров, и ИСПДн.

3.1.4. Местонахождение ПДн определяется, исходя из требований, предъявляемых к форме представления ПДн. Им является:

- сервера баз данных ИСПДн;
- АРМ пользователей ИСПДн;
- съемные/внешние носители, содержащие ПДн;
- твердые копии (бумажные носители), содержащие ПДн.

3.2 Назначение, состав и особенности эксплуатации ИСПДн

3.2.1. По структуре ИСПДн Банка представляют собой многопользовательские автоматизированные системы с разграничением прав доступа.

3.2.2. Доступ к обрабатываемым ПДн осуществляется с использованием технологий удаленного доступа. Все серверы и активное сетевое оборудование,

входящие в состав ИСПДн, располагаются в охраняемых помещениях и находятся в пределах контролируемых зон.

3.2.3. ИСПДн подключены к сети связи общего пользования и международного информационного обмена. Через эти сети осуществляется передача информации, содержащей ПДн клиентов (контрагентов) и работников Банка.

3.2.4. Все технические средства находятся на территории Российской Федерации, трансграничная передача данных не осуществляется.

3.2.5. Состав обрабатываемых в ИСПДн персональных данных:

- ФИО;
- Дата рождения;
- Данные документов, удостоверяющих личность;
- Место рождения;
- Адрес регистрации по месту жительства;
- Адрес фактического проживания;
- Контактные данные;
- Место работы;
- Должность;
- ИНН;

4 Организация защиты персональных данных

4.1 Общие положения

4.1.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

4.1.2. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на Банк.

4.1.3. Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн Банка может назначаться структурное подразделение Банка, должностное лицо (работник) Банка или сторонняя организация, действующая на основании Договора, заключенного между Банком и этой организацией в рамках действующего законодательства РФ, ответственные за обеспечение безопасности ПДн (Уполномоченное лицо).

4.1.4. Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку замысла обеспечения безопасности ПДн;
  - выбор целесообразных способов (мер и средств) защиты ПДн;
  - решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
  - обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в

ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;
- развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;
- доработку СЗПДн по результатам опытной эксплуатации.

4.2 Оценка обстановки

4.2.1 Общие сведения

4.2.1.1. Оценка обстановки основывается на результатах комплексного обследования ИСПДн, в ходе которого, в т.ч., проводится определение защищаемой информации и ее категорирование, а также классификация ИСПДн.

4.2.1.2. Классификация ИСПДн проводится с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

4.2.1.3. При проведении классификации ИСПДн учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- характеристики безопасности персональных данных, обрабатываемых в информационной системе (типовые, специальные информационные системы);
- структура информационной системы (автоматизированные рабочие места, локальные информационные системы, распределенные информационные системы);
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена (системы, имеющие подключения к сетям международного информационного обмена, и системы, не имеющие таких подключений);

- режим обработки персональных данных (однопользовательский, многопользовательский);
- режим разграничения прав доступа пользователей информационной системы (системы без разграничения прав доступа, системы с разграничением прав доступа);
- местонахождение технических средств информационной системы (системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации)

и определяется необходимость обеспечения безопасности ПДн от:

- угроз утечки ПДн по техническим каналам (акустической (речевой) информации, видовой информации, утечка по ПЭМИН);
- угроз уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн;
- угроз хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) в т.ч. с применением программно-аппаратных и программных средств;
- непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

4.2.1.4. При этом учитывается степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн и проводится анализ имеющихся в распоряжении мер и средств защиты ПДн (оценка соответствия ИСПДн требованиям обеспечения безопасности ПДн).

4.2.1.5. Оценка соответствия ИСПДн требованиям обеспечения безопасности ПДн осуществляется в соответствии с документом ФСТЭК России «Положение о методах и способах защиты информации в информационных системах персональных данных» от 5 февраля 2010 г. № 58.

4.2.1.6. Класс информационной системы определяется на основании анализа данных комплексного обследования ИСПДн с учетом частных моделей угроз безопасности персональных данных.

4.2.1.7. Разработка частных моделей угроз осуществляется в соответствии с методическими документами ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 года и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 года.

4.2.1.8. Результатом классификации является присвоение информационным системам соответствующего класса и его документальное оформление.

4.2.2 Организационные требования к проведению классификации ИСПДн

4.2.2.1. Классификация ИСПДн проводится только специально назначаемой комиссией по проведению классификации ИСПДн. Персональный состав комиссии определяется Приказом Председателя Правления Банка.

4.2.2.2. В состав комиссии входят представители следующих подразделений:

- Служба безопасности;
- Управление автоматизации Банка.

При необходимости, возможно привлечение к работе комиссии специалистов других структурных подразделений Банка.

4.2.2.3. Комиссия в своей работе должны руководствоваться следующими нормативными документами:

- «Порядок проведения классификации информационных систем персональных данных», утвержденный приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20;
- методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 года
- методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 года.

4.2.2.4. Результаты классификации информационных систем оформляются соответствующими Актами классификации.

4.2.2.5. Класс информационной системы может быть пересмотрен:

- по решению руководства Банка на основе проведенных Службой безопасности анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной ИСПДн;
- по результатам мероприятий по контролю выполнения требований к обеспечению безопасности персональных данных при их обработке в ИСПДн.

4.2.2.6. Пересмотр класса ИСПДн также осуществляется комиссией по классификации ИСПДн в случаях, указанных в п. 4.2.2.5.

4.3 Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн

4.3.1 Обоснование требований по обеспечению безопасности ПДн

4.3.1.1. Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти, обязательными к применению стандартами, методическими документами ФСТЭК России, а также моделей угроз безопасности ПДн, разрабатываемых в соответствии с методическими документами ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 года и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 года.

4.3.2 Задачи защиты ПДн

4.3.2.1. В соответствии с частной моделью угроз СЗПДн ИСПДн Банка предназначена для решения следующих задач:

- обеспечение целостности данных;
- предотвращение попыток получения НСД к ПДн, обрабатываемых в ИСПДн Банка:
  - путем выявления паролей пользователей;
  - путем перехвата паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой ОС;

- реализуемых стандартными функциями ОС или прикладного программного обеспечения, с применением специально созданных для НСД программ (программ просмотра и модификации реестра, поиска текста в текстовых файлах и т.п.);
- путем анализа сетевого трафика, реализуемого посредством перехвата передаваемой по сети информации внутренним злоумышленником, (обычно путем получения НСД к сетевому оборудованию);
- путем подмены доверенного объекта, реализуемого с помощью подмены объекта в ходе сетевого взаимодействия с целью получения аутентификационных либо других данных;
- путем несанкционированного удаленного запуска приложений;
- путем внедрения вредоносных программ;

- предотвращение угроз сканирования, направленного на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;
- предотвращение отказа в обслуживании, направленного на сетевые сервисы ИСПДн;
- предотвращение несанкционированного, в том числе случайного, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

4.4 Замысел обеспечения безопасности

Замысел обеспечения безопасности ПДн определяет:

- основные направления по защите ПДн;
- выбор способов защиты ПДн;
- вопросы управления защитой ПДн;
- вопросы обеспечения защиты ПДн.

4.4.1 Основные направления по защите ПДн

4.4.1.1. Основным направлением по защите ПДн является обеспечение конфиденциальности при обработке информации, содержащей ПДн, которое обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременным обнаружением фактов несанкционированного доступа к ПДн;
- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянным контролем обеспечения уровня защищенности персональных данных.

4.4.1.2. Обеспечение деятельности по основным направлениям по защите ПДн осуществляет Служба безопасности Банка.

4.4.1.3. Дополнительным направлением по защите ПДн является обеспечение целостности обрабатываемой информации, содержащей ПДн, которое обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного изменения или удаления информации, содержащей ПДн;
- возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.4.1.4. Обеспечение деятельности по дополнительным направлениям по защите ПДн осуществляют подразделения Банка, обеспечивающие функционирование ИС (Управление автоматизации Банка).

4.4.2 Способы защиты ПДн

4.4.2.1. По способам осуществления все меры обеспечения безопасности ПДн при их обработке в ИСПДн подразделяются на правовые, организационные и технические.

4.4.2.2. К правовым мерам относится регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности за нарушение требований указанных законов и актов.

4.4.2.3. К организационным относятся меры, регламентирующие процессы функционирования ИСПДн, порядок использования ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом,

чтобы максимально снизить возможность угроз безопасности ПДн. Организационные меры включают:

- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего ИСПДн;
- организацию охраны и режима допуска к элементам ИСПДн;
- организацию учета, хранения, использования и уничтожения документов и носителей информации, содержащей ПДн.

4.4.2.4. К техническим мерам относятся аппаратные, программные и программно-аппаратные средства защиты, выполняющие (самостоятельно или в комплексе с другими средствами) функции СЗПДн:

- в части защиты от НСД:
  - управление доступом;
  - регистрация и учет;
  - обеспечение целостности;
  - анализ защищенности;
  - обеспечение безопасного межсетевого взаимодействия;
  - обнаружение вторжений;
  - антивирусная защита;
- в части защиты от утечки по техническим каналам:
  - защита акустической (речевой) информации;
  - защита видовой информации;
  - защита от утечки по ПЭМИН.

4.4.3 Основные вопросы управления защитой ПДн

4.4.3.1. Под основными вопросами управления защитой ПДн понимается перечень вопросов, связанных с:

- распределением функций управления доступом к данным и их обработкой между должностными лицами;
- определением порядка изменения правил доступа к защищаемой информации;
- определением порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

- определением порядка действий должностных лиц в случае возникновения нештатных ситуаций;
- определением порядка проведения контрольных мероприятий и действий по его результатам.

4.4.3.2. Распределение обязанностей по основным вопросам управления защитой ПДн при их обработке в ИСПДн, осуществляется следующим образом:

- распределение функций управления доступом к ПДН и их обработкой осуществляется владельцами активов Банка;
- контроль корректности и достаточности осуществляется Службой безопасности Банка.

4.4.3.3. Служба безопасности Банка также осуществляют следующие действия:

- определяет порядок изменения правил доступа к защищаемой информации;
- определяет порядок изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- определяет порядок действий должностных лиц в случае возникновения нештатных ситуаций;
- определяет порядок проведения контрольных мероприятий и действий по его результатам.

4.4.4 Вопросы обеспечения защиты ПДн

Вопросы, связанные с обеспечением замысла защиты ПДн в части финансирования, технической, программной и информационной поддержки распределяются следующим образом:

4.4.4.1. Коллегиальный исполнительный орган - Правление Банка:

- утверждает финансирование программ в области защиты конфиденциальной информации;
- определяет полномочия функциональных подразделений Банка и Службы безопасности Банка в части защиты ПДн.

4.4.4.2. Технический совет Банка:

- определяет техническую политику Банка;
- определяет политику Банка в области информационной безопасности, обеспечивающей повышение эффективности и оперативности работы Банка;

- обеспечивает снижение операционных и технологических рисков на основе современных информационных технологий, путем автоматизации процессов при обеспечении максимально возможного уровня информационной безопасности.

4.4.4.3. Служба безопасности Банка:

- осуществляет методическое обеспечение и информационную поддержку в области защиты ПДн (в рамках задачи обеспечения информационной безопасности Банка);
- организует исполнение пунктов данного Положения (в рамках задачи организации мероприятий и координация работ всех подразделений Банка по комплексной защите на всех этапах технологических циклов создания информации, переноса ее на носитель (бумажный или электронный), обработки и передачи в соответствии с единой политикой обеспечения информационной безопасности);
- организует разработку и выполнение программ в области защиты ПДн;
- осуществляет в пределах своей компетенции проведение проверочных мероприятий в отношении персонала Банка, допущенного к обработке ПДн;
- устанавливает порядок определения размеров ущерба, наступившего из-за несанкционированного, в том числе случайного, доступа к ПДн, результатом которого стало уничтожение, изменение, блокирование, копирование, распространение персональных данных;
- принимает меры по выполнению договоров о совместном использовании и защите ПДн, принимает решения о возможности передачи носителей информации, содержащей ПДн, другим лицам (контрагентам и третьим сторонам) или государственным организациям;
- в пределах своих полномочий решают иные вопросы, возникающие при защите ПДн при их обработке в ИСПДн Банка.

4.4.4.4. Управление автоматизации:

- обеспечивает всестороннюю информационную безопасность Банка;
- обеспечивает бесперебойную и защищенную от несанкционированного доступа работу средств автоматизации и автоматизированных систем.

4.4.4.5. Функциональные структурные подразделения Банка:

- обеспечивают защиту ПДн субъектов, переданных им другими подразделениями (работниками), контрагентами, третьими лицами, учреждениями и организациями;
- обеспечивают защиту ПДн в подчиненных им подразделениях (на личном участке работ) Банка, в соответствии с требованиями нормативно-правовой документации.

4.4.4.6. Подразделения юридического Управления Банка:

- при необходимости инициируют уголовные и гражданские дела о нарушениях при обработке ПДн;
- обеспечивают юридическую защиту подразделений и должностных лиц Банка в связи с их деятельностью по защите ПДн при их обработке в ИСПДн.

4.4.4.7. Руководители структурных подразделений, работники которых имеют доступ к персональным данным, осуществляют контроль защиты персональных данных субъектов ПДн в рамках своих подразделений.

4.4.4.8. Работники Банка обеспечивают конфиденциальность персональных данных субъектов ПДн, ставших им известными в связи с выполнением своих функциональных обязанностей (за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных).

4.5 Планирование мероприятий по защите ПДн

4.5.1. Планирование мероприятий по защите ПДн осуществляется работниками Службы безопасности Банка на основании проведенной классификации ИСПДн и построенных частных моделей угроз, а также результатов предыдущего этапа работ.

4.5.2. Работниками Службы безопасности Банка разрабатывается План (планы) по обеспечению безопасности ПДн, включающий перечень собственно мероприятий, финансовое обеспечение, ответственных и сроки реализации, который согласовывается Коллегиальным исполнительным органом (либо его отдельными представителями) и утверждается Председателем Правления Банка.

4.5.3. Контроль выполнения Плана мероприятий по обеспечению безопасности ПДн возлагается на Управление внутреннего контроля Банка.

4.5.4. Для реализации мероприятий, определяемых Планом по обеспечению безопасности ПДн, возможно привлечение сторонних организаций, имеющих необходимый набор лицензий. В случае принятия положительного решения со

сторонней организацией заключается соответствующий договор, в котором, в т.ч., прописываются обязательства по неразглашению конфиденциальной информации. Далее на указанную организацию распространяются все требования по защите ПДн, действующие в Банке.

4.6 Организация и проведение работ по созданию и поддержке СЗПДн

4.6.1. Под организацией и проведением работ по созданию и поддержке СЗПДн подразумевается комплекс административных и технических мер, направленных на проектирование, внедрение, эксплуатацию и поддержку СЗПДн.

4.6.2. Организацию и проведение работ по созданию и поддержке СЗПДн осуществляет Служба безопасности Банка.

4.6.3. Перечень мероприятий, необходимых для организации и проведения работ по созданию и поддержке СЗПДн определяется в соответствии с требованиями «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного Приказом ФСТЭК России от 5 февраля 2010 г. № 58.

4.6.4. Испытания СЗПДН проводятся в процессе развертывания и ввода в опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн.

4.6.5. По результатам проведения опытной эксплуатации СЗПДн при необходимости проводится доработка системы.

4.6.6. При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн разрабатывается организационно-распорядительная документация по обработке и защите ПДн.

4.6.7. Обязанности по разработке организационно-распорядительной документации по обработке и защите ПДн (за исключением проектов приказов) возложены на Службу безопасности Банка. Разработка проектов приказов осуществляется в соответствии с правилами делопроизводства, принятыми в Банке.

4.6.8. Согласование организационно-распорядительной документации по обеспечению безопасности ПДн (за исключением проектов приказов) производится Юридическим управлением, Управлением автоматизации и, при необходимости, другими подразделениями Банка. Утверждение документации по обеспечению безопасности ПДн осуществляется Председателем Правления Банка.

4.6.9. Пересмотр положений документации по обеспечению безопасности ПДн должен проводиться периодически не реже чем 1 раз в год, а также:

- при изменении используемых технологий работы Банка;
- при изменении Политики информационной безопасности;
- при изменении организационной структуры, структуры информационных и/или телекоммуникационных систем (или введении новых), применении новых технологий передачи, хранения и обработки информации;
- по фактам возникновения инцидентов, уязвимостей, по решению руководства и иных значимых событий ИБ.

4.7 Защита ПДн, находящихся на твердых копиях

4.7.1 При фиксации ПДн на материальном носителе (твердой копии) не допускается фиксация на одном носителе персональных данных, цели обработки которых различны (заведомо не совместимы). Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.7.2 В отношении информации, содержащей ПДн, и находящейся на твердых копиях, выполняются следующие мероприятия:

- хранение твердых копий ПДн, обрабатываемых в ПДн, осуществляется в специальных местах, определенных Службой безопасности Банка и утвержденных руководством Банка;
- доступ к месту хранения твердых копий должен быть ограничен использованием средств физического доступа (кодовые замки, система видеонаблюдения);
- допуск к местам хранения твердых копий ПДн осуществляется на основании списка, утвержденного руководством Банка;
- уничтожение твердых копий ПДн должно осуществляться таким образом, чтобы исключить дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на твердой копии (удаление, вымарывание).

5 Контроль соблюдения условий и правил обработки ПДн и их защиты. Порядок расследований нарушений режимов обработки и защиты ПДн

5.1 Общие положения

5.1.1 Контроль за обеспечением защиты персональных данных осуществляют руководство Банка, Управление внутреннего контроля и Служба безопасности Банка в рамках компетенции в соответствии с действующим законодательством РФ, а также действующими внутренними нормативными документами Банка.

5.1.2 Контроль за соблюдением законодательства РФ при обеспечении защиты ПДн и законностью принимаемых при этом решений осуществляют подразделения юридического Управления Банка.

5.2 Порядок расследования нарушений режимов обработки и защиты ПДн

5.2.1 Расследование нарушений (инцидентов) режимов обработки и защиты ПДн проводится с целью определения ответственных, возмещения причиненного ущерба и предотвращения подобных инцидентов в дальнейшем.

5.2.2 Расследование нарушений[1] осуществляется комиссией[2], в состав которой входят представители Службы безопасности Банка, Управления автоматизиации и структурного подразделения, вовлеченного в инцидент. При необходимости в качестве экспертов могут привлекаться работники других подразделения Банка.

[1] Расследование нарушений (инцидентов) режимов обработки и защиты ПДн в сети и ИС Банка осуществляется в соответствии с «Положением о служебном расследовании нарушений режима информационной безопасности в компьютерной сети и критических приложениях ОАО «ЧЕЛЯБИНВЕСТБАНК».

[2] В случае, если произошел инцидент высокой критичности, по решению руководства Банка для расследования инцидента возможно привлечение правоохранительных органов. В этом случае сбор свидетельств и доказательств по инциденту выполняется сотрудниками правоохранительных органов.

5.2.3 При проведении расследования инцидента, связанного с нарушением требований по защите ПДн, комиссией решаются следующие задачи:

- анализ собранных материалов по нарушению режимов обработки и защиты ПДн и действий по его прекращению;
- определение причин инцидента;
- оценка ущерба;
- определение ответственных за произошедшее;
- решение по привлечению к ответственности;
- определение мер по предотвращению подобных инцидентов в дальнейшем.

5.2.4 Результаты работы комиссии оформляются в виде заключения с рекомендациями, которое утверждается руководством Банка, после чего принимаются меры по недопущению повторения подобных нарушений.

5.2.5 В программу профилактики нарушений входят мероприятия, направленные на:

- доведения до персонала Банка, допущенного до обработки ПДн, всей важности и необходимости выполнения задач по защите ПДн в рамках компетенции персонала Банка;
- проведением плановых и внеплановых проверок с целью выявления нарушений или предпосылок к нарушениям при обработке ПДн;
- доведением, при необходимости, до персонала Банка результатов проведения проверок.

6 Приостановка (отказ) предоставления ПДн

6.1. При обнаружении нарушений порядка предоставления ПДн, Банк незамедлительно приостанавливает предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.