Политика ЗАО ВТБ Специализированный депозитарий по обработке персональных данных

Утверждена приказом ЗАО ВТБ
Специализированный депозитарий
от «19» 08. 2016 г. № 44

Москва 2016

Содержание

Введение

Политика ЗАО ВТБ Специализированный депозитарий по обработке персональных данных (далее - Политика) определяет основные принципы, цели, задачи направления деятельности ЗАО ВТБ Специализированный депозитарий (далее – Общество) в области обработки и защиты персональных данных (далее также - ПДн), оператором которых является Общество.

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон от 27.07.2006 № 152-ФЗ), Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Политика разработана в целях реализации требований законодательства Российской Федерации в области ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн Обществом, в том числе защиты прав на неприкосновенность частной жизни.

Политика определяет стратегию защиты ПДн, обрабатываемых в информационной системе ПДн (далее - ИСПДн) Общества, и формулирует основные принципы и механизмы защиты ПДн.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в ИСПДн Общества.

Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн (далее – СЗПДн), включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии. Технические и программные средства должны соответствовать установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации - возможность получения информации и использования.

Защита информации - принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Использование персональных данных (ПДн) - действия (операции) с ПДн, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц, либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

Конфиденциальность персональных данных (ПДн) - обязанность оператора и иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено Федеральным законом от 27.07. 2006 г. № 152-ФЗ.

Несанкционированный доступ (НСД) - доступ, нарушающий установленные правила разграничения доступа. Лицо, осуществляющее НСД, является нарушителем правил разграничения доступа.

Общество (Оператор ПДн) - Закрытое акционерное общество ВТБ Специализированный депозитарий, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПДн, а также определяющее цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн при осуществлении уставной деятельности, ведении кадрового и бухгалтерского учета.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Ответственный за организацию обработки персональных данных (ПДн) - лицо, уполномоченное Генеральным директором Общества на осуществление действий по организации обработки персональных данных в Обществе, получающее указания непосредственно от Генерального директора Общества и подотчетное ему.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Система защиты персональных данных (СЗПДн) - совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Субъект ПДн - работник Общества или лицо, привлекаемое Обществом для оказания услуг (выполнения работ) по гражданско-правовым договорам, физическое лицо - клиент Общества, а также физическое лицо - представитель юридического лица - клиента или контрагента Общества.

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители персональных данных.

1. Общие положения

1.1. Целью настоящей Политики является обеспечение безопасности ПДн от всех видов угроз, внешних и внутренних, умышленных и не преднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации, а также реализация требований законодательства Российской Федерации в области ПДн.

Основными целями обеспечения безопасности ПДн являются:

- предотвращение нарушений прав субъекта ПДн на сохранение конфиденциальности информации, обрабатываемой в ИСПДн Общества;
- предотвращение искажения или несанкционированной модификации информации, содержащей ПДн, обрабатываемой в ИСПДн Общества;
- предотвращение несанкционированных действий по блокированию информации, содержащей ПДн.

1.2. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

1.3. Внутренние документы Общества, затрагивающие вопросы ПДн, должны разрабатываться с учетом положений Политики и не противоречить им.

1.4. Действие настоящей Политики распространяется на все структурные подразделения и на всех работников Общества (штатных, работающих по договорам гражданско-правового характера и т.п.).

1.5. Настоящая Политика определяет основные цели и задачи, а также общую стратегию построения СЗПДн Общества, в соответствии с Перечнем ИСПДн. Политика определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

1.6. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

1.7. Организационные меры призваны обеспечить:

1.7.1. Конфиденциальность ПДн (защита от несанкционированного ознакомления).

1.7.2. Целостность информации (актуальность и непротиворечивость информации, ее защищенность от уничтожения и несанкционированного изменения).

1.7.3. Доступность информации.

2. Цели обработки персональных данных

2.1. Общество осуществляет обработку персональных данных в следующих целях:

- осуществления и выполнения Обществом функций, полномочий, обязанностей и иной деятельности, предусмотренной уставом и лицензиями Общества, законодательством Российской Федерации, а также нормативными актами Банка России;
- заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных законодательством Российской Федерации и уставом Общества;
- ведения кадровой работы и организации учета работников Общества для обеспечения соблюдения требований нормативных правовых актов Российской Федерации, реализации Обществом обязательств в рамках трудовых отношений, содействия работникам в прохождении обучения, обоснования предоставления работникам различного рода льгот в соответствии с нормативными правовыми актами Российской Федерации;
- исполнения требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц, пенсионного законодательства Российской Федерации при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование;
- обеспечения заполнения первичных учетных документов в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, а также уставом и внутренними документами Общества;
- реализации прав и выполнения обязанностей, предусмотренных законодательством об акционерных обществах (формирование и деятельность органов управления, ведение реестра акционеров, одобрение сделок Общества, размещение акций, распределение прибыли и др.);

• обеспечения личной безопасности работников, обеспечения сохранности имущества, обеспечения безопасности физических лиц и представителей юридических лиц, являющихся контрагентами Общества, посетителей Общества (в случае прохода указанных лиц на территорию Общества), обеспечение безопасности информации, обрабатываемой на объектах и в помещениях Общества.

3. Обрабатываемые персональные данные

3.1. Общество обрабатывает ПДн следующих категорий субъектов ПДн:

• представителей юридического лица, индивидуальных предпринимателей;

• клиентов – физических лиц, заключивших с Обществом договор на депозитарное и/или спецдепозитарное обслуживание;

• контрагентов – физических лиц, заключивших с Обществом договор гражданско-правового характера;

• кандидатов на вакантные должности;

• работников Общества (в т.ч. работников, трудовой договор с которыми прекращен);

• выгодоприобретателей по договорам добровольного страхования жизни работников Общества;

• аффилированных лиц Общества, являющихся физическими лицами.

3.2. Перечень персональных данных, обрабатываемых в Обществе, утверждается приказом Общества. Обработка персональных данных, не включенных в перечень персональных данных, обрабатываемых в Обществе, запрещена.

4. Принципы обработки персональных данных

4.1. Обработка ПДн осуществляется Обществом на основе следующих принципов:

• осуществление обработки на законной и справедливой основе;

• обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

• не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

• недопустимость обработки ПДн, не отвечающих целям их обработки;

• соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки ПДн, недопустимость обработки ПДн, являющихся избыточными по отношению к заявленным целям их обработки;

• обеспечение точности обрабатываемых ПДн, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки ПДн;

• принятие необходимых мер или обеспечение принятия мер по удалению или уточнению неполных или неточных данных;

• хранение персональных данных в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения ПДн не установлен федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

• уничтожение либо обезличивание персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.2. Общество не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также обработку биометрических персональных данных.

4.3. Общество обеспечивает конфиденциальность обрабатываемых персональных данных: не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5. Общие принципы обеспечения защищенности персональных данных

Принцип законности

Проведение защитных мероприятий, реализуемых в Обществе, должно быть организовано в соответствии с законодательством Российской Федерации в области ПДн с применением всех дозволенных методов и средств обнаружения и пресечения нарушений при работе с информацией. Принятые меры защиты не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством Российской Федерации случаях к защищаемой информации.

Принцип системности и комплексности

Системный подход к построению системы защиты ПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения задач по обеспечению безопасности ПДн. При создании СЗПДн должны учитываться все слабые и наиболее уязвимые места информационных систем. Комплексное использование методов и средств защиты предполагает их согласованное применение, перекрывающее все существенные (значимые) атаки при реализации актуальных угроз.

Принцип превентивности

Защита ПДн должна быть нацелена прежде всего на недопущение (пресечение) реализации угроз информационной безопасности, а не на устранение последствий их проявления, которое может потребовать значительных финансовых, временных и материальных затрат, гораздо больших, чем затраты на создание и поддержание работоспособности СЗПДн.

Принцип оптимальности и разумной разнородности

Должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности ПДн. Согласованное применение разнообразных средств при построении целостной системы защиты позволяет минимизировать риск преодоления СЗПДн.

Средства защиты, используемые для обеспечения безопасности ПДн на различных уровнях, должны дублировать основные функции защиты, необходимо организовывать поставку таких средств защиты от разных производителей, что позволяет существенно затруднить процесс преодоления СЗПДн за счет различной логики построения средств защиты.

Принцип непрерывности

СЗПДн должна реализовывать процесс защиты информации непрерывно и целенаправленно, начиная от стадии проектирования и на протяжении всего жизненного цикла ИСПДн.

Принцип адаптивности

СЗПДн должна строиться с учетом возможного изменения конфигурации ИСПДн, числа пользователей. При этом введение каждого нового элемента ИСПДн или изменение действующих условий не должно снижать достигнутый уровень защищенности в целом.

Принцип доказательности и обязательности контроля

При создании СЗПДн должны соблюдаться организационные меры защиты внутри сети, включая привязку логического имени пользователя к определенному рабочему компьютеру, и применение средств идентификации, аутентификации и подтверждения подлинности информации.

СЗПДн должна обеспечивать обязательность и своевременность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.

Принцип конфиденциальности СЗПДн

При построении и использовании СЗПДн должна соблюдаться конфиденциальность реализованных механизмов защиты ПДн. Указанный принцип требует реализации контроля целостности СЗПДн, управления безопасностью через Администратора безопасности ИСПДн, реализации возможности восстановления СЗПДн при отказах оборудования.

Принцип многоуровневости и равнопрочности

СЗПДн должна реализовывать защиту информации на всех уровнях жизнедеятельности ИСПДн (технологическом, пользовательском, локальном, сетевом). Защита должна иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.

Принцип преемственности и совершенствования

СЗПДн должна постоянно совершенствоваться на основе преемственности принятых ранее решений, анализа функционирования ИСПДн и СЗПДн с учетом отечественного и зарубежного опыта в области защиты информации.

Принцип персональной ответственности и минимизации привилегий

СЗПДн должна предусматривать определение прав, обязанностей и ответственности каждого пользователя (в пределах его полномочий) за обеспечение безопасности ПДн. Распределение прав, обязанностей и ответственности должно в случае любого нарушения позволять определить круг виновных.

СЗПДн должны иметь возможность выделять пользователям и администраторам ИСПДн только те права доступа, которые необходимы им для выполнения служебных обязанностей.

6. Задачи системы защиты персональных данных

6.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

6.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

6.2.1. Защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования информационной системой и доступ к ее ресурсам должны иметь только зарегистрированные в установленном порядке пользователи).

6.2.2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;
- аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн.

6.2.3. Регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов.

6.2.4. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

6.2.5. Защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ.

6.2.6. Защиту ПДн от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи.

6.2.7. Защиту ПДн, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения.

6.2.8. Обеспечение функционирования криптографических средств защиты информации при компрометации части ключевой системы.

6.2.9. Своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн.

6.2.10. Создание условий для минимизации и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного воздействия и ликвидация последствий нарушения безопасности ПДн.

7. Меры, методы и средства обеспечения уровня защищенности ПДн

7.1. Обеспечение требуемого уровня защищенности ПДн должно достигаться с использованием мер, методов и средств информационной безопасности.

Меры обеспечения безопасности ИСПДн подразделяются на:

7.1.1. **Законодательные (правовые) меры защиты.** К правовым мерам защиты относятся положения законодательных и иных нормативных правовых актов, регламентирующих правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствующие тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом СЗПДн.

7.1.2. **Организационные и административные меры защиты.** Организационные и административные меры защиты - это меры организационного характера, регламентирующие защиту ПДн, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на уровне Генерального директора Общества - сформировать Политику ЗАО ВТБ Специализированный депозитарий по обработке персональных данных и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения Генерального директора Общества, затрагивающие работу ИСПДн в целом. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн.

7.1.3. **Физические меры защиты.** Физические меры защиты основаны на применении разного рода механических, электро-механических или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7.1.4. **Аппаратно-программные средства защиты ПДн.** Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и

специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.)

7.2. Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

7.3. Контроль может проводиться как Обществом (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

7.4. Контроль может осуществляться Обществом как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

7.5. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

8. Доступ к обрабатываемым персональным данным

8.1. Доступ к обрабатываемым в Обществе ПДн имеют лица, уполномоченные приказом Общества, лица, которым Общество поручило обработку ПДн на основании заключенного договора, а также лица, чьи ПДн подлежат обработке.

8.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством Российской Федерации функции Общества закрепляются за соответствующими структурными подразделениями Общества.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Общества, могут иметь только работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих работников.

8.3. Доступ работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних документов Общества.

Допущенные к обработке ПДн работники под роспись знакомятся с документами Общества, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных работников.

8.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Обществом, определяется в соответствии с законодательством Российской Федерации и устанавливается внутренними документами Общества.

9. Реализуемые требования к защите персональных данных

9.1. Общество принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

9.2. Состав указанных в пункте 9.1 Политики мер, включая их содержание и выбор средств

защиты ПДн, определяется, а внутренние документы об обработке и защите ПДн утверждаются Обществом исходя из требований:

- Федерального закона от 27.07.2006 г. № 152-ФЗ;
- главы 14 Трудового кодекса Российской Федерации;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

9.3. В предусмотренных законодательством Российской Федерации случаях обработка ПДн осуществляется Обществом с согласия субъектов ПДн.

Обществом производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

9.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения не установлен Федеральным законом от 27.07.2006 № 152-ФЗ или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

9.5. Обществом осуществляется ознакомление работников Общества, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, Политикой и иными внутренними документами по вопросам обработки ПДн, и (или) обучение работников по вопросам обработки и защиты ПДн.

9.6. При обработке ПДн с использованием средств автоматизации Обществом, в частности, применяются следующие меры:

- назначается Ответственный за организацию обработки ПДн и определяется его компетенция;
- назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе;
- утверждаются внутренние документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;
- осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Федеральному закону от 27.07.2006 № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним документам Общества;
- проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ, определяется соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение исполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ.

9.7. Обеспечение безопасности ПДн в Обществе при их обработке в ИСПДн достигается, в частности, путем:

- определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства Российской Федерации и с учетом проведения оценки возможного вреда;

• определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Обществом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки СЗПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

• применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Обществе, в том числе, осуществляются:

• организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

• установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

• оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

• учет машинных носителей ПДн, обеспечение их сохранности;

• обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

• восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

8.8. Обеспечение защиты ПДн в Обществе при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

• обособления ПДн от иной информации;

• недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

• использования отдельных материальных носителей для обработки каждой категории ПДн;

• принятия мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

• соблюдения требований:

–к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

–уточнению ПДн;

–уничтожению или обезличиванию части ПДн;

–использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

–ведению журналов, содержащих ПДн, необходимых для выдачи однократных пропусков субъектам ПДн в занимаемые Обществом здание и помещения;

–хранению ПДн, в том числе к обеспечению раздельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

10. Требования к работникам по обеспечению защиты персональных данных

10.1. Все работники Общества, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

10.2. При вступлении в должность нового работника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

10.3. Работник должен быть ознакомлен с положениями настоящей Политики, а также с процедурами работы с элементами ИСПДн и СЗПДн.

10.4. Работники Общества, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

10.5. Работники Общества должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

10.6. Работники Общества должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

10.7. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

10.8. Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Общества, третьим лицам.

10.9. При работе с ПДн в ИСПДн работники Общества обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест АРМ или терминалов.

10.10. При завершении работы с ИСПДн работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

10.11.Работники Общества должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

11. Ответственность

Работники Общества, разгласившие персональные данные субъектов ПДн, работники, по вине которых произошло нарушение конфиденциальности ПДн, и работники, создавшие предпосылки к нарушению конфиденциальности ПДн, несут ответственность, предусмотренную законодательством Российской Федерации, внутренними документами Общества и условиями трудового договора.

12. Пересмотр Политики

Внесение изменений в Политику может быть вызвано изменениями в ИСПДн, системе защиты ПДн, изменениями нормативных правовых актов и иных документов.

Внесению изменений в Политику предшествуют:

- обследование и анализ изменений в ИСПДн и СЗПДн;
- анализ изменений нормативных правовых актов и иных документов;
- вносятся изменения в Политику информационной безопасности ПДн;
- вносятся изменения в документы, регламентирующие конкретные направления деятельности по обеспечению безопасности ПДн.