Общество с ограниченной ответственностью
«ДС Генератор»

ОГРН 1182375050670, ИНН 2370008248, КПП 237001001
Юридический адрес: 353561, Краснодарский край, Славянский район г. Славянск-на Кубани, ул. Красная д. 156Б офис 501
Почтовый адрес: 350015, Краснодарский край г. Краснодар ул. Новокузнечная д. 67
+7(962)-882-14-28; e-mail: m.baeva@danycom.ru

УТВЕРЖДЕНО:
Генеральный директор
ООО «ДС Генератор»

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации и в информационных системах персональных данных ООО «ДС Генератор»

Редакция 1

Славянск-на-Кубани, 2018

СОДЕРЖАНИЕ

1. Назначение Положения

Положение о персональных данных ООО «ДС Генератор» разработано на основе и во исполнение ст. 23 и ст. 24 Конституции РФ, главы 14 Трудового кодекса РФ, Федерального закона РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г., Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 15.09.08 №687, Постановления Правительства от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», других нормативных правовых актов и в развитие внутренних актов ООО «ДС Генератор».

Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению защиты персональных данных, работников, клиентов и контрагентов, обрабатываемых ООО «ДС Генератор».

2. Термины и сокращения

АРМ	Автоматизированное рабочее место
БД	Базы данных
ВП	Вредоносная программа
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ЛВС	Локально-вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПМВ	Программно-математические воздействия
ПЭВМ	Персональная электронно-вычислительная машина
РФ	Российская Федерация
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СЗПДн	Система (подсистема) защиты персональных данных
ФЗ	Федеральный закон

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с Перечнем присвоенных идентификаторов.

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.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных - действия (операции) с персональными данными, 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 работника или других лиц.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Материальный носитель персональных данных (далее материальный носитель) – материальный объект, используемый для закрепления и хранения информации. В целях настоящего Положения под материальным носителем понимается бумажный документ, диск, дискета, флэш-карта и т.п.

Неавтоматизированная обработка персональных данных – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из Субъектов ПДн осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту ПДн.

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 ПДн персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект информатизации – совокупность информационных ресурсов, содержащих ПДн, средств и систем, обрабатывающих ПДн, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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.

Пользователь - сотрудник ООО «ДС Генератор», работающий по трудовому договору, а также специалисты, оказывающие услуги (выполняющие работы) для ООО «ДС Генератор» на основании гражданско-правового договора, а также представители юридических лиц, имеющих с ООО «ДС Генератор» договорные отношения (подрядчики, аудиторы и т.п.), зарегистрированные в ИСПДн ООО «ДС Генератор» в установленном порядке и получивших право на доступ к ресурсам ИСПДн в соответствии с функциональными обязанностями и/или полномочиями, установленными договором с ООО «ДС Генератор».

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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.

Ресурс информационной системы – именованный элемент системного прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъект персональных данных – (потенциальный) работник ООО «ДС Генератор», (потенциальный) клиент ООО «ДС Генератор», контрагент ООО «ДС Генератор», член органа управления ООО «ДС Генератор», иное физическое лицо, обработка персональных данных которого производится ООО «ДС Генератор».

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Цель обработки персональных данных – конкретный конечный результат действий, совершенных с персональными данными, вытекающий из требований законодательства и направленный, в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон.

3. Область применения

Положение является внутренним нормативным документом ООО «ДС Генератор», регламентирующим деятельность в сфере обработки и защиты ПДн. Требования Положения обязательны для выполнения всеми пользователями ООО «ДС Генератор», допущенными к работе с ПДн, а также обеспечивающими защиту ПДн.

4. Общие положения

Настоящее Положение определяет состав и порядок обработки персональных данных работников ООО «ДС Генератор» и иных лиц, чьи ПДн обрабатываются ООО «ДС Генератор».

Настоящее Положение разработано в целях соблюдения законодательства, сохранения неприкосновенности частной жизни, в том числе, в целях обеспечения защиты персональных данных. ПДн всегда являются конфиденциальной, строго охраняемой информацией.

Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

Выполнение мероприятий по защите ПДн позволяет обеспечить защиту прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну.

Защита ПДн в ООО «ДС Генератор» достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

Объектами защиты в ООО «ДС Генератор» являются ПДн, средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства изготовления, тиражирования документов и другие технические средства обработки информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), используемые для обработки ПДн.

Положение подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке персональных данных.

Все пользователи ООО «ДС Генератор», обрабатывающие ПДн, должны быть ознакомлены с настоящим Положением под подпись.

5. Нормативные ссылки

5.1. Внешние

1. Конституция Российской Федерации.
2. Трудовой кодекс Российской Федерации.
3. Федеральный Закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный Закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Указ Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

6. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
7. Постановление Правительства от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
8. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
9. «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», утверждена Заместителем директора ФСТЭК России 15.02.2008 г.
10. «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утверждена Заместителем директора ФСТЭК России 15.02.2008 г.
11. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21.02.2008 г.
12. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утверждены руководством 8 Центра ФСБ России 21.02.2008 г.
13. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6. Понятие и состав ПДн

Под ПДн субъектов ПДн понимается информация, необходимая ООО «ДС Генератор» в связи с трудовыми отношениями и касающаяся конкретного работника, а также информация, относящаяся к физическому(-им) лицу(-ам) (клиентам, контрагентам) и необходимая ООО «ДС Генератор» для выполнения договорных обязательств.

Субъектами ПДн, обработка ПДн которых осуществляется ООО «ДС Генератор», являются:

- работники ООО «ДС Генератор»;
- физические лица, состоящие в договорных отношениях с ООО «ДС Генератор» (далее клиент);
- физические лица, являющиеся выгодоприобретателями, не состоящие в договорных отношениях с ООО «ДС Генератор» (далее клиент);
- физические лица, являющиеся представителями юридических лиц, состоящих в договорных отношениях с ООО «ДС Генератор» (далее клиент);
- посетители ООО «ДС Генератор».

Целями получения и обработки ПДн работников являются организация учета персонала ООО «ДС Генератор», обеспечение соблюдения законов и иных нормативно-правовых актов, содействие служащему в трудоустройстве, обучении, продвижении по службе, пользовании различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных».

Целью получения и обработки ПДн клиентов является выполнение условий (обязанностей) договора и/или осуществление возложенных на ООО «ДС Генератор» законодательством Российской Федерации функций в соответствии нормативными правовыми актами Российской Федерации в области связи, в том числе Федеральным законом от 07.07.2003 г. №126-ФЗ «О связи», Федеральным законом от 13.03.2006 г. № 38-ФЗ «О рекламе» и др.

Целью получения и обработки ПДн посетителей является оформление и учет пропусков посетителей на территорию ООО «ДС Генератор».

При определении объема и содержания, обрабатываемых ПДн субъектов, ООО «ДС Генератор» руководствуется целям получения и обработки ПДн.

Информационные ресурсы, содержащие ПДн субъектов, создаются путём:

- копирования оригиналов документов, содержащих ПДн (например, паспорт, страховое свидетельство государственного пенсионного страхования);
- внесения сведений в учётные формы на бумажных носителях (например, личная карточка по форме Т-2);
- внесения сведений в базы данных;
- получения оригиналов необходимых документов (например, трудовая книжка, автобиография, анкета, заявления).

Состав обрабатываемых ПДн субъектов утверждается приказом ООО «ДС Генератор».

7. Права и обязанности ООО «ДС Генератор»

Обработка ПДн должна осуществляться с письменного согласия субъекта ПДн. Форма согласия на обработку ПДн приведена в Приложении 1 к настоящему Положению. ООО «ДС Генератор» обязано разъяснить субъекту ПДн последствия отказа предоставить свои ПДн.

Согласие субъекта ПДн на обработку ПДн не требуется в следующих случаях, предусмотренных частью 2 статьи 6 ФЗ «О персональных данных»:

- обработка ПДн осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПДн и круг субъектов, ПДн которых подлежат обработке, а также определяющего полномочия оператора;
- обработка ПДн необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является субъект ПДн;
- обработка ПДн осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПДн;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами связи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
- обработка ПДн осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- осуществляется обработка ПДн, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПДн лиц, замещающих государственные должности, должности государственной гражданской службы, ПДн кандидатов на выборные государственные или муниципальные должности.

ООО «ДС Генератор» обязано обеспечивать конфиденциальность ПДн, за исключением случаев обезличивания и в отношении общедоступных ПДн.

ПДн субъектов, обрабатываемые ООО «ДС Генератор» могут быть включены в общедоступные источники ПДн только с письменного согласия субъекта ПДн. Форма согласия на внесение ПДн в общедоступные источники приведена в Приложении 2 к настоящему Положению.

Получение ПДн у третьих лиц должно осуществляться только с письменного согласия субъекта ПДн. Форма согласия на получение ПДн у третьих лиц приведена в Приложении 3 к настоящему Положению.

ООО «ДС Генератор» обязано безвозмездно предоставить субъекту возможность ознакомления с его ПДн по его просьбе (письменному запросу) информацию, касающуюся обработки его ПДн. Форма письменного запроса субъекта приведена в Приложении 4 к настоящему Положению. Форма письменного ответа субъекту ПДн об обрабатываемых ПДн субъекта приведена в Приложении 5 к настоящему Положению.

В случаях, если ПДн были получены не от субъекта ПДн, ООО «ДС Генератор» до начала обработки ПДн обязано уведомить субъекта ПДн и сообщить ему следующую информацию:

- наименование и адрес ООО «ДС Генератор»;
- цель обработки ПДн и ее правовое основание;
- права субъекта ПДн.

Форма уведомления субъекта ПДн о начале обработке его ПДн приведена в Приложении 6 к настоящему Положению.

В случае отзыва субъектом согласия на обработку своих ПДн ООО «ДС Генератор» обязано прекратить обработку ПДн и уничтожить ПДн. Форма отзыва согласия приведена в Приложении 7 к настоящему Положению.

В случае выявления недостоверных ПДн или неправомерных действий с ними ООО «ДС Генератор» обязано блокировать ПДн.

В случае подтверждения факта недостоверности ПДн субъекта ООО «ДС Генератор» обязано уточнить ПДн и снять их блокирование.

В случае выявления неправомерных действий с ПДн ООО «ДС Генератор» обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений ООО «ДС Генератор» обязано уничтожить ПДн.

Об устранении допущенных нарушений или об уничтожении ПДн ООО «ДС Генератор» обязано уведомить субъекта ПДн, а также тех лиц, которым ПДн этого субъекта были переданы, в письменной форме согласно Приложению 8 к настоящему Положению.

В случае достижения цели обработки ПДн ООО «ДС Генератор» обязано незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта ПДн в письменной форме.

8. Права и обязанности субъектов ПДн

Субъекты ПДн принимают решение о предоставлении своих ПДн и дают согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 статьи 9 ФЗ «О персональных данных». Форма согласия на обработку ПДн приведена в Приложении 1 к настоящему Положению.

Субъект ПДн может отозвать согласие на обработку ПДн. Форма отзыва согласия на обработку ПДн приведена в Приложении 7 к настоящему Положению.

Субъекты ПДн имеют право на получение сведений об ООО «ДС Генератор», о месте его нахождения, о наличии своих ПДн, а также на ознакомление с такими ПДн.

Субъекты ПДн имеют право на получение сведений, касающихся обработки своих ПДн. Форма направляемого запроса об обрабатываемых ПДн приведена в Приложении 4 к настоящему Положению.

Субъекты ПДн имеют право требовать исключения или исправления неверных или неполных ПДн, а также данных, обработанных с нарушением требований законодательства. Форма направляемого запроса об исключении из обработки или исправлении неверных ПДн, а также данных, обработанных с нарушением законодательства, приведена в Приложении 9 к настоящему Положению.

В случае получения от субъекта запроса на прекращение обработки ПДн уполномоченный сотрудник ООО «ДС Генератор» обязан разъяснить субъекту его права и указать возможность выполнения условия соглашения с ним без обработки его ПДн.

Субъекты ПДн имеют право требовать от ООО «ДС Генератор» извещать всех лиц, которым ранее были сообщены неверные или неполные ПДн, обо всех произведенных исключениях, исправлениях или дополнениях в указанных сведениях.

Субъекты ПДн имеют право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке. Субъекты ПДн имеют право обжаловать в суде любые неправомерные действия или бездействие ООО «ДС Генератор» при обработке и защите его ПДн.

9. Сбор ПДн

ПДн субъекта следует получать у самого субъекта ПДн. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие, в котором указываются: цель, предполагаемые источники и способы получения ПДн, а также сведения о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на получение ПДн.

ООО «ДС Генератор» не имеет права собирать и обрабатывать ПДн о политических, религиозных и иных убеждениях и частной жизни субъекта ПДн. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации ООО «ДС Генератор» вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

ООО «ДС Генератор» не имеет права собирать и обрабатывать ПДн о членстве субъекта ПДн в Общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законом.

9.1. Сбор ПДн работников ООО «ДС Генератор»

При заключении трудового договора работник предоставляет ООО «ДС Генератор» в соответствии со ст. 65 Трудового кодекса РФ сведения о себе:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

В отдельных случаях, с учетом специфики работы Трудовым кодексом, иными Федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

Работник дает письменное согласие на обработку и передачу своих ПДн при приеме на работу.

ООО «ДС Генератор» проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами. Предоставление работником подложных документов или ложных сведений при поступлении на работу может являться основанием для расторжения трудового договора.

Личное дело работника оформляется после заключения с ним трудового договора и издания приказа о приеме на работу. Все документы личного дела подшиваются в обложку установленного образца. На ней указываются фамилия, имя, отчество работника, номер личного дела. Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитых в личное дело, нумеруются. Личное дело ведется на протяжении всей трудовой деятельности работника. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами. Личное дело считается завершенным при увольнении работника и сдается в архив на хранение.

9.2. Сбор ПДн клиентов

Клиент предоставляет ООО «ДС Генератор» ПДн, объем и характер которых соответствует целям получения и обработки ПДн в ООО «ДС Генератор». ООО «ДС Генератор» начинает обработку ПДн клиента только после получения от него письменного согласия.

10. Доступ к ПДн

10.1. Доступ к ПДн должностных лиц ООО «ДС Генератор»

Доступ к ПДн, подлежащим автоматизированной и неавтоматизированной обработке, разрешен только должностным лицам, допущенным к работе с ПДн ООО «ДС Генератор».

Генеральный директор ООО «ДС Генератор» по представлению руководителей структурных подразделений определяет Приказом, лиц из числа пользователей ООО «ДС Генератор», уполномоченных на обработку ПДн граждан, обрабатывающих ПДн в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных», других нормативных правовых актов Российской Федерации и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих ПДн, а также подписывают Обязательство о неразглашении ПДн ООО «ДС Генератор» (по форме согласно Приложению 10 к настоящему Положению).

Пользователи ООО «ДС Генератор», получившие доступ к ПДн, принимают обязательства по обеспечению конфиденциальности обрабатываемых ПДн, которые определены:

- трудовым договором;
- обязательством о неразглашении ПДн;
- должностными инструкциями в части обеспечения безопасности ПДн.

Доступ должностных лиц к информационным системам и связанным с их использованием работам (операциям с ПДн), осуществляется в соответствии с требованиями п. 13.3.2.3.2 настоящего Положения.

Доступ должностных лиц к материальным носителям ПДн и местам их хранения определяется в соответствии с Перечнем мест хранения материальных носителей ПДн, утверждаемым Приказом генерального директора ООО «ДС Генератор».

10.2. Доступ к ПДн органов государственной власти

Доступ к ПДн органам государственной власти предоставляется в случаях, предусмотренных Федеральными законами, в том числе:

- в целях предупреждения угрозы жизни и здоровья субъекта ПДн;
- в целях защиты основ конституционного строя, нравственности, прав и законных интересов других лиц;
- в целях обеспечения обороны страны и безопасности государства, в том числе при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях».
- Доступ к ПДн на основании и во исполнение Федеральных законов, предоставляется:
- Федеральной инспекции труда и федеральным органам исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности;
- Федеральной налоговой службе и межрегиональным инспекциям и управлениям ФНС РФ по субъектам РФ;
- Федеральной службе государственной статистики и её территориальным органам;
- Федеральному фонду обязательного медицинского страхования и его территориальным органам;

- Военным комиссариатам;
- Фонду социального страхования РФ;
- Пенсионному фонду РФ.

10.3. Доступ к ПДн третьих лиц

Сторонние организации и/или третьи лица для получения доступа к ПДн обязаны предоставить в письменной форме запрос (Приложение 11 к настоящему Положению), подписанный руководителем организации и заверенный печатью и/или личной подписью третьего лица.

В случае принятия решения о предоставлении доступа к ПДн субъекта организации и/или третьему лицу, ООО «ДС Генератор» направляет ответ о предоставлении информации в письменной форме согласно Приложению 12 к настоящему Положению.

Сторонние организации и/или третьи лица для получения доступа к ПДн подписывают Соглашение о конфиденциальности ПДн (по форме согласно Приложению 13 к настоящему Положению), если обязанность о неразглашении конфиденциальной информации не предусмотрена (не является) условием договора.

В случае отказа в предоставлении организации и/или третьему лицу доступа к ПДн, ООО «ДС Генератор» направляет мотивированный ответ в письменной форме согласно Приложению 12 к настоящему Положению, содержащий ссылку на положение ч. 5 ст. 14 ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа.

ПДн могут быть предоставлены родственникам или членам семьи только с письменного согласия субъекта ПДн.

Обращения (запросы) на предоставления доступа к обрабатываемым ПДн, с отметкой о предоставлении информации по запросу или отказе в предоставлении, фиксируется в соответствующем журнале учета обращений субъектов ПДн (Приложение 14 к настоящему Положению).

11. Передача ПДн

Передача ПДн третьим лицам (юридическим и/или физическим лицам) возможна только с письменного согласия субъекта ПДн. В письменном согласии субъекта ПДн должна быть указано третье лицо (юридическое лицо и/или физическое лицо), которому передаются ПДн, а также цель передачи и обработки ПДн.

При передаче ПДн организациям, физическим лицам, которые на основании договоров осуществляют обработку ПДн, в порядке, установленном законодательством РФ, ООО «ДС Генератор» ограничивает эту информацию только теми ПДн, которые необходимы для выполнения указанными лицами их функций (услуг, работ).

ООО «ДС Генератор» предоставляет (передает) сведения, содержащие ПДн субъектов в Пенсионный фонд РФ, Федеральную налоговую службу по телекоммуникационным каналам связи и, в соответствии с требованиями законодательства, используя криптографические средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн.

Передача ПДн субъектов в пределах ООО «ДС Генератор» возможна только тем сотрудникам, которые допущены к работе с ПДн.

Передача ПДн субъекту возможна только по письменному заявлению субъекта. ООО «ДС Генератор» обязано не позднее трех рабочих дней со дня подачи этого заявления выдать субъекту копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, о периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться субъекту безвозмездно.

Передача (распространение) информации, содержащей ПДн клиентов, должно осуществляться в закрытом виде (в запечатанных конвертах) или иным способом, обеспечивающим ее конфиденциальность.

При передаче ПДн субъекта должны соблюдаться следующие требования:

- не сообщать ПДн субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных действующим законодательством РФ;
- не сообщать ПДн субъекта в коммерческих целях без его письменного согласия. Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с предварительного согласия субъекта ПДн;
- предупреждать лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие ПДн, обязаны соблюдать режим конфиденциальности;
- разрешать доступ к ПДн только специально уполномоченным на это пользователям, при этом указанные пользователи должны иметь право получать только те ПДн, которые необходимы для выполнения ими должностных обязанностей;
- передавать ПДн субъектов их представителям в порядке, установленном действующим законодательством РФ, и ограничивать эту информацию только

теми ПДн, которые необходимы для выполнения указанными представителями их должностных функций;

- передача ПДн внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- трансграничная передача ПДн на территорию иностранного государства допускается без согласия субъекта, если на его территории обеспечивается адекватная защита ПДн.

12. Хранение и уничтожение ПДн

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

ПДн подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

В обязательном порядке устанавливается срок хранения ПДн и осуществляется регулярное уничтожение, а также обезличивание ПДн при наличии такой возможности.

Черновые редакции документов, испорченные бланки документов, листы со служебными записями должны быть уничтожены в машине для уничтожения бумаг.

Материальные носители ПДн должны быть уничтожены после достижения целей обработки ПДн и/или по истечении срока хранения ПДн. Форма Акта уничтожения носителей ПДн приведена в Приложении 15 к настоящему Положению.

13. Обеспечение безопасности ПДн ООО «ДС Генератор»

13.1. ПДн, подлежащие защите в ООО «ДС Генератор»

Актуализация перечня ПДн, обрабатываемых в ООО «ДС Генератор» осуществляется Департаментом экономической и информационной безопасности с учетом действующего «Перечня персональных данных, обрабатываемых в ООО «ДС Генератор» и утверждается приказом Генерального директора ООО «ДС Генератор».

Информационные ресурсы, содержащие ПДн, определяются «Перечнем защищаемых ресурсов ИСПДн», который утверждается приказом Генерального директора ООО «ДС Генератор».

Информационные ресурсы, содержащие ПДн, расположены в ИСПДн ООО «ДС Генератор», состоящих из автоматизированных рабочих мест (АРМ) пользователей на базе ПЭВМ, серверах и съемных носителях информации.

В целях информационного обеспечения ООО «ДС Генератор» могут создаваться общедоступные источники ПДн (в том числе справочники, телефонные книги, адресные книги). Режим конфиденциальности для общедоступных источников ПДн не устанавливается.

ПДн, обработка которых осуществляется без использования средств автоматизации, обособляются от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

13.2. Обеспечение безопасности ПДн при обработке, осуществляемой без использования средств автоматизации

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель (например, отдельные анкеты).

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, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих

ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, имя (наименование) и адрес, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;
- типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

ООО «ДС Генератор» обязано обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

ООО «ДС Генератор» обязано обеспечить сохранность ПДн путем установления мер, исключающих несанкционированный доступ к ПДн. К таким мерам относятся:

- ограничение перечня лиц, имеющих право доступа и обработки ПДн, и уровня доступа;
- ведение учета выданных ПДн, ведение журнала и учет выданных ПДн возлагается на сотрудников Департамента по организации и обеспечению документооборота;
- реализация особого режима хранения для документов, содержащих ПДн Субъектов.

Должно обеспечиваться раздельное хранение ПДн, обработка которых осуществляется в различных целях, в соответствии с перечнем мест хранения материальных носителей ПДн, утверждаемым Генеральным директором ООО «ДС Генератор».

Должен обеспечиваться учет:

- выдачи материальных носителей ПДн (Приложение 16 к настоящему Положению);
- материальных носителей ПДн (Приложение 17 к настоящему Положению).

При ведении журналов оформления и учета пропусков посетителей на территорию ООО «ДС Генератор» должны соблюдаться следующие условия:

- фиксация в журнале информации, запрашиваемой у субъектов ПДн,

осуществляется сотрудниками, имеющими доступ к материальным носителям и ответственными за ведение и сохранность журнала.

- копирование содержащейся в таких журналах информации не допускается.
- ПДн каждого субъекта ПДн могут заноситься в журнал не более одного раза в каждом случае пропуска субъекта ПДн на территорию ООО «ДС Генератор».

Пользователям, работающим с ПДн запрещается оставлять на рабочем столе документы, содержащие ПДн, если в данный момент они с ними не работают. Исполняемые документы не разрешается хранить в россыпи, а должны быть сформированы в папки, на которых указывается вид производимых с ними действий (подшивка в личные дела, для отправки и пр.).

ООО «ДС Генератор» вправе определить дополнительные меры в целях обеспечения сохранности ПДн и исключения несанкционированного доступа к ПДн в своих локальных актах или Приказах Генерального директора.

ООО «ДС Генератор» проводит ознакомление пользователей с нормативными правовыми актами и актами ООО «ДС Генератор» в области защиты ПДн, в том числе в случае их изменения; разъясняет права, обязанности и ответственность пользователей за нарушение норм в данной области.

13.3. Обеспечение безопасности ПДн при обработке, при их обработке в ИСПДн

13.3.1. Порядок классификации ИСПДн и оценки угроз безопасности ПДн при их обработке в ИСПДн

Классификация ИСПДн проводится в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Классификация ИСПДн проводится на этапе создания ИСПДн или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн.

ИСПДн классифицируются с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и средств защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств защиты зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн.

Класс специальной информационной системы определяется на основе модели угроз безопасности ПДн в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

По результатам классификации ИСПДн оформляется акт классификации, утверждаемый Генеральным директором ООО «ДС Генератор».

Класс ИСПДн может быть пересмотрен:

- по решению комиссии по классификации на основе проведенного анализа и

оценки угроз безопасности ПДн с учетом особенностей и (или) изменений конкретной ИСПДн;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в информационной системе.

Выбор и реализация методов и способов защиты ПДн в ИСПДн осуществляются на основе определяемых ООО «ДС Генератор» угроз безопасности ПДн (оформленных в виде частной модели угроз) и в зависимости от класса ИСПДн.

Выбранные и реализованные методы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в информационных системах в составе создаваемой ООО «ДС Генератор» (уполномоченным лицом) системы защиты ПДн.

Выявление угроз ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе экспертного метода, в том числе путем опроса специалистов, персонала ИСПДн, должностных лиц, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

Частная модель угроз безопасности ПДн при их обработке в ИСПДн разрабатывается на основе руководящих документов ФСТЭК: «Методики определения актуальных угроз безопасности ПДн при их обработке в информационных системах персональных данных» и «Базовой модели угроз безопасности ПДн при их обработке в информационных системах ПДн». Частная модель угроз безопасности ПДн в ООО «ДС Генератор» должна периодически пересматриваться в соответствии с «Планом внутренних проверок состояния защиты ПДн».

При использовании средств криптографической защиты информации в ИСПДн для каждой такой ИСПДн должна быть разработана Модель нарушителя безопасности ПДн. Модель нарушителя разрабатывается на основе Методических рекомендаций по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации ФСБ России. На основе выработанной модели нарушителя для каждой ИСПДн определяется уровень криптографической защиты ПДн, которому должно соответствовать применяемое средство криптографической защиты.

13.3.2. Требования по защите ПДн при их обработке в ИСПДн

ООО «ДС Генератор» должно соблюдать режим конфиденциальности при обработке ПДн, за исключением случаев, когда обеспечение конфиденциальности ПДн не требуется.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

Методы защиты информации от несанкционированного доступа, обеспечивающие функции управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы определяются оператором (уполномоченным лицом) в соответствии с утвержденными приказом ФСТЭК России от 18 февраля 2013 г. №21 «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Методами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

При обработке ПДн в ИСПДн ООО «ДС Генератор» должны соблюдаться следующие требования безопасности:

- ограничение состава пользователей и регламентация их функциональных обязанностей, для выполнения которых требуется доступ к ПДн;
- применять средства защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- вести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
- осуществлять контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- должна обеспечиваться возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

13.3.2.1. Порядок разработки, ввода в действие и эксплуатации ИСПДн

Для защиты ПДн в ИСПДн должны разрабатываться система защиты персональных данных (СЗПДн). Конкретные требования (технические и организационные) по защите ПДн для каждой ИСПДн должны формироваться в виде «Технического задания на создание СЗПДн в ИСПДн». В случае, если требования к ИСПДн разрабатываются сторонней организацией, обязательным требованием является наличие у этой организации лицензии на выполнение работ по технической защите конфиденциальной информации ФСТЭК России. Требования должны формироваться на

основании положений руководящих документов ФСТЭК и ФСБ, перечень которых приведен в п. 5 настоящего Положения.

Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн, устанавливаются следующие стадии создания СЗПДн:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на создание СЗПДн;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в её составе;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случае, если:

- изменился состав обрабатываемых ПДн;
- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменился состав угроз безопасности ПДн в ИСПДн;
- изменился класс ИСПДн.

Для каждой ИСПДн разрабатывается и поддерживается в актуальном состоянии перечень используемых средств защиты информации (средств криптографической защиты информации) в соответствии с формами, приведенными в Приложениях 18, 19 к настоящему Положению.

Используемые средства защиты должны подвергаться тестированию в соответствии с документацией на средства защиты. Результаты тестирования отражаются в журнале периодического тестирования средств защиты информации. Форма журнала приведена в Приложении 20, к настоящему Положению.

13.3.2.2. Порядок оценки соответствия ИСПДн требованиям безопасности ПДн

Оценка соответствия ИСПДн классов К1 требованиям безопасности ПДн проводится в виде декларирования соответствия / аттестации на соответствие требованиям безопасности информации.

Оценка соответствия ИСПДн классов К2 требованиям безопасности ПДн проводится в виде декларирования соответствия / аттестации на соответствие требованиям безопасности информации.

Оценка соответствия ИСПДн классов К3 требованиям безопасности ПДн проводится в виде декларирования соответствия / аттестации на соответствие требованиям безопасности информации.

Для ИСПДн класса К4 оценка соответствия не проводится.

В случае изменения условий и технологии обработки ПДн в аттестованных ИСПДн руководители структурных подразделений ООО «ДС Генератор», участвующих в обработке ПДн, обязаны известить ответственного за защиту ПДн в ООО «ДС Генератор». Ответственный за защиту ПДн, на основании анализа полученной информации принимает решение об уведомлении органа по аттестации и внесении изменений в документацию на ИСПДн. Орган по аттестации принимает решение о необходимости проведения дополнительной проверки эффективности обеспечения безопасности ПДн с учетом внесенных изменений.

Для ИСПДн, оценка соответствия которых произведена в виде декларирования соответствия, необходимо выполнять следующие требования:

- руководители структурных подразделений, участвующих в обработке ПДн,

должны уведомлять ответственного за защиту ПДн в ООО «ДС Генератор» об изменениях технологий обработки ПДн;

- Ответственный за защиту ПДн, на основании анализа полученной информации принимает решение о необходимость проведения повторного декларирования соответствия ИСПДн и внесения изменений в документацию на ИСПДн;
- декларирование соответствия всех ИСПДн в ООО «ДС Генератор» должно проводится на периодической основе не реже чем 1 раз в год.

При проведении мероприятий по обеспечению безопасности ПДн привлекаемый внешний исполнитель должен обладать лицензией ФСТЭК на осуществление деятельности по технической защите конфиденциальной информации.

13.3.2.3. Организационные меры по защите ПДн при их обработке в ИСПДн

13.3.2.3.1. Требования к оборудованию помещений и рабочих мест пользователей ИСПДн

Все технические средства ИСПДн ООО «ДС Генератор» должны находиться в пределах контролируемых зон, исключающих неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

При размещении АРМ пользователей ИСПДн на нижних этажах зданий их рекомендуется располагать во внутренних помещениях, максимально удаленных от границ контролируемых зон.

Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обслуживанием оборудования.

Размещение устройств отображения и печати информации, используемых в составе АРМ пользователей ИСПДн ООО «ДС Генератор», должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами. Кроме того, должны приниматься дополнительные меры, исключающие подобный просмотр (шторы, жалюзи на окнах, непрозрачные экраны).

Неиспользуемые в процессе обработки ПДн устройства ввода/вывода АРМ пользователей ИСПДн (COM, LPT, НГМД, CD, USB) необходимо отключить либо опечатать (опломбировать) в случае, если данные функции нельзя реализовать с помощью СЗИ на программном уровне.

Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельной опломбированной комнате с прочной запираемой дверью. Перечень лиц, имеющих право доступа в указанные помещения, утверждаются приказом Генерального директора ООО «ДС Генератор». Ключи от дверей данных помещений должны быть только у лиц, имеющих право доступа в них. Допускается устанавливать коммуникационное оборудование в отдельных запираемых и опечатываемых металлических шкафах, размещаемых в охраняемых помещениях.

13.3.2.3.2. Требования к процедуре получения доступа в ИСПДн

Предоставление доступа к ПДн, обрабатываемым в ИСПДн осуществляется на основании заявки руководителя структурного подразделения сотрудника. Форма заявки приведена в Приложении 21 к настоящему Положению. Заявка согласовывается с Департаментом информационно-аналитического обеспечения.

Заявка хранится в течение всего времени, пока пользователю предоставлен доступ к ПДн и в течение 1 года с момента окончания предоставления доступа.

Администратором безопасности ИСПДн должна проводиться периодическая проверка прав пользователей ИСПДн.

Проверка прав пользователей[1] должна проводиться на периодической основе или после каждого изменения в системе. При этом проверка прав пользователей, имеющих особые привилегии для доступа в систему должна проводиться с меньшей периодичностью.

Должна быть предусмотрена регулярная проверка адекватности назначенных привилегий с целью исключения получения кем-либо из пользователей излишних прав.

13.3.2.4. Технические требования по защите ПДн при их обработке в ИСПДн

Технические требования по защите ПДн при их обработке в ИСПДн, обеспечивающие реализацию подсистем управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия в зависимости от класса информационной системы устанавливаются в соответствии с утвержденными приказом ФСТЭК России от 18 февраля 2013 г. №21 «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

13.3.2.4.1. Требования к резервированию

Для обеспечения возможности быстрого восстановления ПДн и средств их обработки, в случае повреждения (утраты) рабочей копии, в ИСПДн ООО «ДС Генератор» должны выполняться следующие требования:

- резервные копии информационных ресурсов, содержащих ПДн, и инструкции по их восстановлению должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;
- для обеспечения сохранности резервных копий должен быть применён комплекс организационных и технических мер защиты;
- носители, на которые осуществляется резервное копирование, должны регулярно проверяться на работоспособность;
- должны быть предусмотрены регулярные проверки процедур восстановления.

[1] Под «проверкой прав пользователей» понимается проверка соответствия полномочий пользователей, определенных Заявкой на предоставление доступа, с действующими правами доступа, указанными в учетной записи пользователя, к информационным ресурсам ИСПДн ООО «ДС Генератор»

14. Планирование и контроль обеспечения безопасности ПДн

Планирование работ по защите информации проводится в целях выявления и устранения недостатков в системе защиты информации, разработки предложений по ее совершенствованию. Планирование осуществляется заместителем директора Департаментов информационно-аналитического обеспечения ООО «ДС Генератор».

В ООО «ДС Генератор» разрабатывается утверждаемый Генеральным директором или его заместителем План мероприятий по защите ПДн, включающий следующие основные мероприятия:

- разработку (модернизацию) систем защиты информации;
- контроль защищенности информации в ИСПДн;
- контроль организации защиты информации;
- устранение недостатков по результатам ранее проведенных проверок и контрольных мероприятий.

План включает в себя перечень мероприятий, подразделения, ответственные за проведение работ, сроки выполнения мероприятий и состав отчетных документов, оформляемых по результатам их реализации. План мероприятий по защите ПДн разрабатывается ежегодно.

Выполнение ежегодно плана оформляется в виде журнала учета мероприятий по защите информации в ИСПДн (Приложение 22 к настоящему Положению).

С целью своевременного выявления и предотвращения утечки информации, содержащей ПДн, в ИСПДн должен проводиться периодический (не реже 1 в год) контроль состояния защиты ПДн, который заключается в оценке:

- соблюдения требований руководящих и нормативно-методических документов по защите ПДн;
- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;
- знаний и выполнения пользователями своих функциональных обязанностей в части защиты ПДн.

Контроль осуществляется путем проведения плановых и внеплановых проверок. Плановые проверки пользователей ИСПДн, технических средств и систем проводятся комиссиями, назначаемыми приказом Генерального директора ООО «ДС Генератор». Внеплановые проверки проводятся по усмотрению заместителя директора Департамента информационно-аналитического обеспечения, директора Департамента информационно-аналитического обеспечения, Генерального директора ООО «ДС Генератор», а также руководителей территориальных подразделений ООО «ДС Генератор».

План внутренних проверок состояния защиты ПДн в ИСПДн составляется на 12 месяцев по форме, приведенной в Приложении 23 к настоящему Положению.

Результаты работы комиссии по проверке оформляются актом в произвольной форме, утверждаемым генеральным директором ООО «ДС Генератор». В Акте указываются рекомендации по закрытию возможных каналов утечки информации.

Проверка технических средств и систем проводится не реже одного раза в год, а также дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

Все работы по контролю должны проводиться при строгом соблюдении мер безопасности, исключающих разглашение сведений о проводимых работах, местах размещения технических средств и систем, используемых СЗИ и возможных каналах утечки информации, содержащей ПДн.

Ответственность за соблюдение режима безопасности при проведении проверок выполнения требований по защите ПДн возлагается на ответственного за проведение проверки в соответствии с формой, приведенной в Приложении 23 к настоящему Положению.

В случаях обнаружения нарушений при обработке ПДн в ИСПДн ООО «ДС Генератор» ответственный за защиту ПДн обязан:

- немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;
- организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается только после устранения нарушений и проверки достаточности и эффективности принятых мер, соответствия их требованиям нормативных документов по защите ПДн.

15. Проверки регулирующими органами

В соответствии с требованиями ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора), муниципального контроля» проверки проводятся в соответствии с утвержденными административными регламентами.

Информация о порядке проведения проверок предоставляется:

- посредством размещения на официальном сайте Роскомназдора в сети общего доступа Интернет
- непосредственно в центральном аппарате Роскомназдора и ее территориальных органах.

Срок проведения, как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней. В исключительных случаях, связанных с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований на основании мотивированных предложений должностных лиц Роскомназдора или его территориального органа, проводящих выездную плановую проверку, срок проведения выездной плановой проверки может быть продлен руководителем Роскомназдора или руководителем территориального органа Роскомназдора, но не более чем на двадцать рабочих дней.

Вопросы обеспечения безопасности ПДн при их обработке в ИСПДн, а также требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн находятся в компетенции Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Внеплановые проверки могут проводятся по следующим основаниям:

- истечение срока исполнения ООО «ДС Генератор» ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области ПДн.
- поступление в Роскомнадзор или ее территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:
  - возникновение угрозы причинения вреда жизни, здоровью граждан;
  - причинение вреда жизни, здоровью граждан;
- нарушение прав потребителей (в случае поступления в адрес Роскомназдора или ее территориального органа обращений и заявлений граждан и (или) юридических лиц по вопросам, связанным с нарушением прав потребителей при предоставлении ООО «ДС Генератор» услуги, в рамках которой осуществляется обработка ПДн).

О проведении внеплановой выездной проверки ООО «ДС Генератор» уведомляется Роскомназдором или его территориальным органом не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом. Если в результате деятельности ООО «ДС Генератор» причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление ООО «ДС Генератор» о начале проведения внеплановой выездной проверки не требуется.

При проведении проверки (плановой или внеплановой) от ООО «ДС Генератор» назначается ответственный за сопровождение проверки. Ответственный является официальным представителем ООО «ДС Генератор» при проведении проверок.

Все проверки ООО «ДС Генератор» по вопросам обработки и защиты ПДн должны учитываться в Журнале учета проверок, проводимых органами государственного

контроля (надзора), органами муниципального контроля (Приложение 24 к настоящему Положению).

16. Ответственность

Пользователи, виновные в нарушении нормативных правовых актов и внутренних актов ООО «ДС Генератор», регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

ООО «ДС Генератор», как Оператор ПДн в пределах, установленных законом, несет ответственность за использование ПДн в целях причинения имущественного и морального вреда Субъектам ПДн, затруднения реализации их прав и свобод. Ограничение прав Субъектов ПДн на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.