УТВЕРЖДАЮ
Генеральный директор
ООО «Витте Про»
_____ Пугачев М.А.
«__» _____ 2020 г.
Экз. №____

ПОЛОЖЕНИЕ

об организации обработки и обеспечении безопасности персональных данных в ООО «Витте Про»

г.Москва

Оглавление

1 Права и распространение

1.1 Все права интеллектуальной собственности принадлежат:

ООО «Витте Про» © 2020 г.

1.2 Распространение копий допускается по согласованию с разработчиками документа. Оригиналы в электронном виде и в виде утвержденных печатных копий находятся под контролем библиотек и архивов разработчиков документа. Передача копий третьим лицам не допускается.

1.3 Информация о документе

Наименование документа:	Положение об организации обработки и обеспечении безопасности персональных данных в ООО «Витте Про»

2 Общие положения

2.1 О документе

2.1.1 Настоящее «Положение об организации обработки и обеспечении безопасности персональных данных в ООО «Витте Про» (далее – Положение) определяет порядок обработки и обеспечения безопасности персональных данных субъектов персональных данных в ООО «Витте Про» (далее – Оператор, Компания).

2.1.2 Положение разработано в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2.1.3 Положение обязательно для исполнения всеми лицами, непосредственно осуществляющими обработку и защиту персональных данных в Операторе. Нарушение порядка обработки и защиты персональных данных, определённого Положением, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

2.1.4 Положение вступает в силу после его утверждения руководителем Оператора. Все изменения в Положение вносятся на основании решения руководителя Оператора в установленном порядке.

2.1.5 Положение распространяется, в том числе, на обработку обезличенных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

2.1.6 Все персональные данные, обрабатываемые Оператором, за исключением обезличенных данных и персональных данных, сделанными общедоступными субъектом персональных данных, признаются информацией ограниченного доступа.

2.2 Список сокращений и аббревиатур

2.2.1 В Положении используются следующие сокращения и аббревиатуры:

БД	База данных
ГК РФ	Гражданский кодекс Российской Федерации
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ИСПДн	Информационная система персональных данных
КоАП РФ	Кодекс об административных правонарушениях Российской Федерации
НСД	Несанкционированный доступ
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
ПО	Программное обеспечение
П-21	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. приказом ФСТЭК России от 18.02.2013 № 21)
П-346	Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных» (утв. приказом Минкомсвязи РФ от 21.12.2011 № 346)
ПП-1119	Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 01.11.2012 № 1119)
ПП-687	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15.09.2008 № 687)
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации (уполномоченный орган по защите прав субъектов персональных данных)
РФ	Российская Федерация
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
СЗПДн	Система защиты персональных данных
ТК РФ	Трудовой кодекс Российской Федерации
УК РФ	Уголовный кодекс Российской Федерации
ФСБ России	Федеральная служба безопасности Российской Федерации (федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности)
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации (федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации)
149-ФЗ	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
294-ФЗ	Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при

осуществлении государственного контроля (надзора) и муниципального контроля»

2.3 Список понятий и определений

2.3.1 В Положении используются следующие основные понятия и определения:

Автоматизированная обработка ПДн	Обработка ПДн с помощью средств вычислительной техники.
БД	Совокупность данных, хранимых в соответствии со схемой данных, манипулирование которыми выполняют в соответствии с правилами средств моделирования данных.
Биометрические ПДн	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.
Блокирование ПДн	Временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
Доступ к ПДн	Возможность получения ПДн и их использования.
Запись ПДн	Ввод ПДн в электронную вычислительную машину и (или) фиксация ПДн на материальном носителе.
Изменение ПДн	Действия, направленные на модификацию значений ПДн.
Извлечение ПДн	Действия, направленные на построение структурированных ПДн из неструктурированных или слабоструктурированных машиночитаемых документов.
Информация	Сведения (сообщения, данные) независимо от формы их представления.
Информационная система	Совокупность содержащейся в БД информации и обеспечивающих ее обработку информационных технологий и технических средств.
ИСПДн	Совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
Информационный поиск ПДн	Действия, методы и процедуры, позволяющие осуществлять отбор определенных ПДн из массива данных.
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
Использование 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 информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
Материальный носитель информации (носитель документированной информации)	Материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в т.ч. в преобразованном виде.
Накопление ПДн	Действия, направленные на формирование исходного, несистематизированного массива ПДн.

Неавтоматизированная обработка ПДн (обработка ПДн без использования средств автоматизации)	Обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы, если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека. Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн либо были извлечены из нее.
Обезличенные данные	Данные, хранимые в ИС в электронном виде, принадлежность которых конкретному субъекту ПДн невозможно определить без дополнительной информации.
Обезличивание ПДн	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
Обновление ПДн	Действия, направленные на приведение записанных ПДн в соответствие с состоянием отображаемых объектов предметной области.
Обработка ПДн	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 ПДн.
Обработчик ПДн	Лицо, осуществляющее обработку ПДн по поручению оператора.
Общедоступные источники ПДн	Содержащиеся в информационных системах или зафиксированные на материальных носителях ПДн, доступ неограниченного круга лиц к которым предоставлен с письменного согласия субъекта этих ПДн.
Оператор [ПДн]	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.
Оператор ИСПДн	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации ИСПДн, в т.ч. по обработке ПДн, содержащихся в ее БД. Если иное не установлено федеральными законами, оператором ИСПДн является собственник технических средств, используемых для обработки содержащихся в БД ПДн, который правомерно пользуется такими БД, или лицо, с которым этот собственник заключил договор об эксплуатации ИСПДн.
ПДн	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
ПДн, сделанные общедоступными субъектом	ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.
Передача ПДн	Распространение, предоставление или доступ к ПДн.
Помещение	Часть объема здания или сооружения, имеющая определенное назначение и ограниченная строительными конструкциями, в которой: осуществляется обработка ПДн; размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой,

	аутентифицирующей и парольной информации СКЗИ.
Предоставление ПДн	Действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.
Программно-техническая база ИСПДн	Программные и технические средства серверной части ИСПДн, включая системное (в т.ч. операционная система), прикладное (в т.ч. система управления базами данных) и специальное программное обеспечение.
Раскрытие ПДн	Обеспечение доступа к ПДн неограниченного круга лиц независимо от цели получения указанных ПДн.
Распространение ПДн	Действия, направленные на раскрытие ПДн неопределенному кругу лиц.
Сбор ПДн	Действия, направленные на получение персональных данных непосредственно от субъекта этих данных или его представителя.
СЗПДн	Совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.
СКЗИ	Аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.
Систематизация ПДн	Действия, направленные на объединение и расположение ПДн в определенной последовательности.
Специальные категории ПДн	ПДн, в т.ч., касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости.
Техническое средство	Изделие, оборудование, аппаратура или их составные части, функционирование которых основано на законах электротехники, радиотехники и (или) электроники, содержащие электронные компоненты и (или) схемы, которые выполняют одну или несколько следующих функций: усиление, генерирование, преобразование, переключение и запоминание.
Удаление ПДн	Изъятие ПДн из информационных систем с сохранением последующей возможности их восстановления.
Уничтожение ПДн	Действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.
Уточнение ПДн	Действия, направленные на обновление или изменение ПДн.
Хранение ПДн	Действия, направленные на неизменность состояния материального носителя ПДн.

2.4 Общие положения по организации обработки и обеспечению безопасности ПДн

2.4.1 Необходимость формирования порядка организации обработки и обеспечения безопасности ПДн обусловлена требованиями действующих нормативных правовых актов, устанавливающих обязанности по соответствию объема и содержания, обрабатываемых ПДн заявленным целям сбора, уточнению, хранению и уничтожению ПДн, соблюдению условий обработки ПДн, в том числе получению согласия субъектов на обработку их ПДн, установлению схем взаимодействия как внутри Компании, так и с субъектами ПДн, третьими лицами, регуляторами (уполномоченными органами).

2.4.2 Одним из элементов указанного порядка в части вопросов организации обработки ПДн является лицо, ответственное за организацию обработки ПДн. Указанное лицо назначается в установленном порядке, и в его основные обязанности входит, в том числе:

(1) осуществление внутреннего контроля за соблюдением законодательства о ПДн, в том числе требований к их защите;

(2) доведение до сведения сотрудников Компании положений законодательства РФ в области ПДн, локальных актов по вопросам обработки ПДн, требований к их защите;

(3) организация приема и обработки обращений и запросов субъектов ПДн или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

2.4.3 Разрабатывается система локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ в области ПДн, устранение последствий таких нарушений.

2.4.4 Разрабатывается и размещается в свободном доступе документ, определяющий политику Компании в отношении обработки и защиты ПДн.

2.4.5 Проводится оценка возможного вреда субъектам ПДн в связи с возможным нарушением прав и законных интересов субъекта ПДн (далее – оценка вреда) определённых действующим законодательством РФ в области ПДн, а также соотносит возможный вред субъектам ПДн с реализуемыми мерами.

2.4.6 Направляется в Роскомнадзор уведомление об обработке ПДн. В случае изменения сведений, содержащихся в уведомлении, а также в случае прекращения обработки ПД также производится уведомление об этом Роскомнадзор. Форма уведомления об обработке (о намерении осуществлять обработку) ПДн, а также форма информационного письма о внесении изменений в сведения об Операторе в реестре операторов, осуществляющих обработку ПДн, установлены П-346.

2.4.7 Сотрудники, непосредственно осуществляющие обработку ПДн, знакомятся с положениями законодательства РФ в области ПДн, в том числе требованиями к защите ПДн, локальными актами по вопросам обработки ПДн, а также проходят инструктаж об изменении требований законодательства РФ в области ПДн.

2.4.8 Обеспечение безопасности ПДн, обрабатываемых в ИСПДн, осуществляется в соответствии с требованиями ПП-1119, а также в соответствии с требованиями нормативных актов ФСТЭК России и ФСБ России.

2.4.9 Выполнение требований законодательства РФ в области организации

обработки ПДн контролируется лицом, ответственным за организацию обработки ПДн, либо комиссией, формируемой в установленном порядке, посредством проведения внутреннего контроля.

2.4.10 В случае выявления нарушений требований законодательства РФ в области ПДн Компания проводит служебное расследование. По результатам служебного расследования возможно привлечение к ответственности:

(1) лица, ответственного за организацию обработки ПДн, – к дисциплинарной, административной (ст.ст.5.39, 13.11, 13.14, 19.7 КоАП РФ), гражданско-правовой (возмещение морального, имущественного вреда, понесенных субъектом ПДн убытков) или уголовной (ст.ст.137, 140 УК РФ) ответственности;

(2) сотрудников, осуществляющих обработку ПДн, – к дисциплинарной (ст.192 ТК РФ РФ), материальной (глава 39 ТК РФ), административной (ст.ст.5.27, 13.14 КоАП РФ), гражданско-правовой (возмещение морального, имущественного вреда, понесенных субъектом ПДн убытков) или уголовной (ст.137 УК РФ) ответственности.

2.5 Построение СЗПДн

2.5.1 Построение СЗПДн необходимо в случае осуществления обработки ПДн в ИСПДн и регламентируется:

(1) ПП-1119, которое определяет необходимость и порядок создания СЗПДн, оперируя при этом понятием «оператор ИСПДн», на которого оно и возлагает обязанности по созданию СЗПДн;

(2) П-21, который описывает процедуру определения состава и содержания технических и организационных мероприятий в рамках СЗПДн;

(3) иными нормативными актами ФСТЭК России и ФСБ России.

2.5.2 Для каждой ИСПДн определяется лицо, являющееся её оператором. Согласно 149-ФЗ, оператором ИСПДн является лицо, осуществляющее деятельность по эксплуатации ИСПДн, в том числе по обработке информации, содержащейся в её БД. При этом оператором ИСПДн является собственник используемых для обработки содержащейся в БД информации технических средств, которые правомерно используются такими БД, или лицо, с которым этот собственник заключил договор об эксплуатации данной ИСПДн.

2.5.3 При определении лица, осуществляющего эксплуатацию ИСПДн, помимо прав собственности на технические средства, необходимо также учесть положения законодательства об авторском праве, в соответствии с которыми эксплуатацию невозможно осуществлять без обладания неисключительными правами на программное обеспечение. Кроме того, в состав ИСПДн входят также технические и

программные средства, с помощью которых производится доступ в ИСПДн третьими лицами. Таким образом, для определения лица, осуществляющего эксплуатацию ИСПДн, необходимо исходить из наличия прав собственности на программно-техническую базу ИСПДн.

2.5.4 Определение оператора ИСПДн осуществляется следующим способом:

(1) если программно-техническая база ИСПДн принадлежат одному лицу, при этом это лицо не имеет договора, в котором оно поручало бы эксплуатацию данной ИСПДн другому лицу, то оно является оператором данной ИСПДн;

(2) если лицо осуществляет эксплуатацию ИСПДн в соответствии с договором, заключённым с лицом, являющимся владельцем программно-технической базы ИСПДн, то оно является оператором данной ИСПДн;

(3) если программно-техническая база ИСПДн принадлежит разным лицам, между этими лицами должен быть заключен договор, по которому одно из этих лиц или третье лицо осуществляет эксплуатацию ИСПДн. Лицо, осуществляющее эксплуатацию ИСПДн, и будет являться оператором данной ИСПДн.

2.5.5 СЗПДн создается для каждой ИСПДн. СЗИ, применяемые при создании одной СЗПДн, могут одновременно использоваться и в других СЗПДн. Оператор ИСПДн выполняет следующую последовательность действий:

(1) Оператор ИСПДн использует ранее проведенную оценку вреда (см. п.2.4.5 Положения). Если в ИСПДн обрабатываются ПДн по поручению других операторов, Оператор ИСПДн, наряду с собственной оценкой вреда, использует оценку вреда каждого из вышеуказанных операторов;

(2) Оператор ИСПДн в соответствии с ПП-1119 делает вывод о типе угроз, и определяет актуальные угрозы для ИСПДн, определяет необходимый уровень защищенности;

(3) исходя из типов актуальных угроз для ИСПДн и совокупной оценки вреда, полученной от всех операторов, по поручению которых производится обработка ПДн в ИСПДн, Оператор ИСПДн определяет необходимый уровень защищённости ПДн при их обработке в ИСПДн;

(4) Оператор ИСПДн определяет требования к созданию СЗПДн, опираясь на требования П-21, выполняя поочерёдно следующие этапы:

(4.1) определяется базовый набор мер по обеспечению безопасности ПДн для установленного уровня защищенности ПДн в соответствии с П-21;

(4.2) базовый набор мер адаптируется с учетом структурно-функциональных характеристик ИСПДн, информационных технологий, особенностей функционирования ИСПДн;

(4.3) проводится уточнение адаптированного базового набора мер с учетом не выбранных ранее мер, по результатам которого определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности ПДн для конкретной ИСПДн;

(4.4) уточненный адаптированный базовый набор мер дополняется мерами, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации;

(5) адаптация базового набора мер и уточнение адаптированного базового набора мер производится Оператором ИСПДн с учётом уровня централизации сервисов информационного обеспечения и других особенностей информационной инфраструктуры. При этом для отдельных выбранных мер по обеспечению безопасности ПДн техническая реализация может быть признана невозможной, либо они могут быть признаны экономически нецелесообразными на основании оценки потенциального вреда субъектам ПДн при реализации угроз, исключаемых данными мерами. Вышеуказанные отдельные меры заменяются компенсирующими мерами, направленными на нейтрализацию данных актуальных угроз безопасности ПДн, в том числе и с использованием СЗИ, прошедших процедуру оценки соответствия в форме, отличной от сертификации;

(6) Оператор ИСПДн самостоятельно или с привлечением третьих лиц готовит техническое описание СЗПДн, отвечающее ранее определённым требованиям;

(7) Оператор ИСПДн осуществляет подготовительные мероприятия (в том числе, закупку СЗИ, обучение администраторов и т.д.) и производит ввод в эксплуатацию СЗПДн.

2.6 Организация внутреннего контроля

2.6.1 В целях осуществления внутреннего контроля за соблюдением обязательных требований в сфере обработки и защиты ПДн, а также в рамках соблюдения требований п.4 ч.1 ст.18¹ 152-ФЗ и п.17 ПП-1119, Компанией регулярно проводятся следующие проверки:

(1) соответствия обработки ПДн в структурных подразделениях Компании требованиям законодательства РФ в области ПДн;

(2) актуальности и соответствия законодательству имеющихся организационно-распорядительных документов в области обработки ПДн;

(3) актуальности перечня обрабатываемых ПДн;

(4) актуальности перечня ИСПДн;

(5) актуальности перечня лиц, участвующих в обработке ПДн;

(6) актуальности прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей;

(7) актуальности предоставленной в Роскомнадзор информации об обработке ПДн;

(8) знания сотрудниками Компании законодательства РФ в области ПДн, порядка обработки ПДн и поддержания режима защиты ПДн в части их касающейся;

(9) текущего состояния технических мер по защите ПДн в соответствии с действующим законодательством РФ в области ПДн;

(10) текущего состояния мер по соблюдению прав субъектов ПДн в соответствии с законодательством РФ в области ПДн.

2.6.2 При проведении внутренних проверок в Компании применяются необходимые требования (контроли) действующего законодательства РФ в области ПДн (см. раздел 2.9 Положения).

2.6.3 План внутренних проверок разрабатывается с учетом статуса и важности проверяемых процессов, подлежащих контролю, а также результатов предыдущих проверок. Отбор лиц, осуществляющих проверки, и процедура проверки должны обеспечивать объективность и беспристрастность внутреннего контроля. Проверяющие не должны проводить проверку своей собственной работы.

2.6.4 По результатам проведения каждой проверки лицом, ответственным за организацию обработки ПДн (либо комиссией, формируемой в установленном Компанией порядке) составляется акт внутренней проверки условий обработки ПДн, а в случае выявленных нарушений – также и отчет служебного разбирательства по факту каждого выявленного нарушения.

2.6.5 Руководитель структурного подразделения, ответственный за проверяемый участок деятельности Компании, должен своевременно и без задержки обеспечить проведение проверки результатов устранения обнаруженных ранее несоответствий и их причин. Последующие действия должны включать в себя проверку предпринятых действий и сообщение о результатах проверки.

2.6.6 Все правила и требования, относящиеся к планированию, проведению внутреннего контроля и сообщению о его результатах в Компании, должны быть документированы.

2.7 Прохождение и содержание проверок (государственного надзора)

2.7.1 Содержание мероприятий по контролю и надзору за соблюдением прав субъектов ПДн, проводимых уполномоченными органами, а также сложившаяся судебная практика в сфере ПДн позволяют сделать вывод о важности корректного применения нормативных требований Оператором, а также о необходимости четкой

организации взаимодействия между сотрудниками Оператора при осуществлении проверок. Существующие нормативные правовые акты, регламентирующие порядок осуществления контроля и надзора, устанавливают также права проверяемых организаций и определенные ограничения для проверяющих, знание которых также имеет немаловажное значение при подготовке к проверкам.

2.7.2 Полномочиями по обеспечению контроля и надзора за соответствием обработки ПДн требованиям 152-ФЗ наделен Роскомнадзор, который в ходе проведения проверки рассматривает документы Оператора (уведомление об обработке ПДн, письменные согласия субъектов ПДн, документы, подтверждающие уничтожение ПДн Оператором по достижении цели обработки и т.д.), а также осуществляет обследование ИСПДн в части, касающейся ПДн, обрабатываемых в них.

2.7.3 Оператором устанавливается порядок действий сотрудников при получении информации о предстоящей проверке (в зависимости от вида – плановая или внеплановая), а также при получении запросов от Роскомнадзора и иных уполномоченных органов (ФСТЭК России, ФСБ России и т.д.). Мониторинг информации о включении в план проверок Оператора осуществляется лицом, ответственным за организацию обработки ПДн.

2.7.4 Правила и требования, относящиеся к порядку взаимодействия Оператора с Роскомнадзором и иными уполномоченными органами, должны быть документированы.

2.7.5 До начала проведения проверки лицо, ответственное за организацию обработки ПДн, проводит инструктаж с сотрудниками Оператора о предстоящем взаимодействии с проверяющими в части тех процессов обработки ПДн, в которых они принимают участие. В ходе проведения проверки лицо, ответственное за организацию обработки ПДн, осуществляет контроль за тем, чтобы с проверяющими взаимодействовали именно те сотрудники Оператора, которые прошли инструктаж.

2.7.6 В ходе проведения проверки лицо, ответственное за организацию обработки ПДн, сопровождает проверяющих совместно с сотрудником подразделения, ответственного за обеспечение соблюдения законности у Оператора и юридическую защиту его интересов. В случае получения замечаний от проверяющих Оператор инициирует их устранение до момента окончания проверки.

2.7.7 Лицо, ответственное за организацию обработки ПДн, осуществляет контроль соответствия хода проверки положениям соответствующих нормативно правовых актов П-312, в частности необходимо:

(1) не допускать проведение проверки при отсутствии руководителя Оператора (иного уполномоченного представителя), за исключением случая, когда проверка проводится по основанию причинения вреда жизни и здоровью граждан;

(2) осуществлять контроль за представлением проверяющим исключительно той информации/документов, которые относятся к предмету проверки;

(3) не допускать изъятия проверяющими оригиналов документов.

2.7.8 Лицо, ответственное за организацию обработки ПДн, осуществляет контроль устранения замечаний, полученных от проверяющих в ходе проведения проверки, до момента ее окончания.

2.7.9 Оператором организуется обсуждение результатов проведения проверки с целью фиксации и дальнейшего использования полученного опыта взаимодействия с Роскомнадзором и иными уполномоченными органами.

2.7.10 В случае получения предписания об устранении выявленных нарушений по результатам проведенных проверок Оператор осуществляет уведомление уполномоченного органа об осуществлении их устранения.

2.8 Улучшение порядка управления и обеспечения обработки и защиты ПДн

2.8.1 Оператор на регулярной основе улучшает порядок управления и обеспечения обработки и защиты ПДн с учетом регулярных изменений требований действующего законодательства РФ и характеристик процессов организации обработки и обеспечения безопасности ПДн, а также по причине выработки новых подходов и практик обработки и защиты ПДн.

2.8.2 Улучшение достигается посредством уточнения (пересмотра) Положения, использования результатов внутреннего контроля и проверок (государственного надзора), корректирующих и предупреждающих действий.

2.8.3 Положение пересматривается на регулярной основе – не реже одного раза в год с момента проведения предыдущего пересмотра Положения. Положение заново утверждается, если по результатам пересмотра в Положение вносятся изменения.

2.8.4 Положение может пересматриваться и заново утверждаться ранее срока, указанного в п.2.8.3 Положения, по мере внесения изменений в нормативные правовые акты в сфере ПДн. Все изменения в Положение вносятся в соответствии с разработанным в Компании СТО СМК-ДП.423.02 «Управление документацией».

2.8.5 Оператор проводит мероприятия по устранению причин несоответствий требованиям действующего законодательства РФ в области ПДн и локальных актов с целью предупредить их повторное возникновение.

2.8.6 Оператор определяет действия, необходимые для устранения причин потенциальных несоответствий требованиям действующего законодательства РФ в области ПДн и локальных актов Оператора, с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать размеру вреда, который может быть причинен Оператору.

2.8.7 Затраты на проведение мероприятий по предотвращению несоответствий более экономичны, чем на корректирующие действия.

2.8.8 Критически важным для улучшения порядка управления и обеспечения обработки и защиты ПДн являются состав, квалификация и опыт лиц, привлекаемых к данной активности.

2.8.9 Состав лиц, участвующих в улучшении порядка управления и обеспечения обработки и защиты ПДн:

(1) лицо, ответственное за организацию обработки ПДн;

(2) лицо, ответственное за обеспечение безопасности ПДн в ИСПДн, или представитель структурного подразделения Оператора, ответственного за обеспечение безопасности ПДн в ИСПДн;

(3) представитель структурного подразделения Оператора, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Оператора;

(4) представитель структурного подразделения Оператора, ответственного за ведение кадрового учета;

(5) представитель структурного подразделения Оператора, ответственного за документационное обеспечение управления;

(6) в некоторых ситуациях необходимо привлечение третьих лиц (сторонних организаций), обладающих соответствующими компетенциями.

2.8.10 Квалификация и опыт лиц, участвующих в улучшении порядка управления и обеспечения обработки и защиты ПДн, должны соответствовать поставленной перед ними задаче. Указанные лица в своей совокупности должны:

(1) знать требования действующего законодательства РФ о ПДн;

(2) обладать как минимум базовыми знаниями в сфере управления и обеспечения информационной безопасности;

(3) иметь достаточно длительный опыт работы в организации, являющейся Оператором.

2.9 Контроли несоответствий и рекомендации по устранению несоответствий

2.9.1 С целью повышения эффективности и результативности мероприятий внутреннего контроля Компании над соблюдением обязательных требований в сфере обработки и защиты ПДн (см. раздел 2.6 Положения) в Положении закреплен перечень требований (контролей) действующего законодательства РФ в области ПДн. С практической точки зрения проверка выполнения каждого из контролей позволит лицам, осуществляющим мероприятия внутреннего контроля, составить полное и

обоснованное мнение о фактическом выполнении Оператором требований законодательства о ПДн.

2.9.2 Нижеприведенные 68 контролей можно условно разделить на две категории:

(1) контроли несоответствий требованиям действующего законодательства РФ в области ПДн, указанные в п.п.1-27, связаны непосредственно с процессами обработки ПДн;

(2) контроли несоответствий требованиям действующего законодательства РФ в области ПДн, указанные в п.п.28-68, связаны с операционной деятельностью по управлению и обеспечению безопасности обработки ПДн.

2.9.3 Каждому из контролей соответствует определенный перечень санкций (мер юридической ответственности за несоблюдение требований законодательства РФ в области ПДн) и приведен перечень типовых рекомендаций по устранению выявленных несоответствий, который применим по отношению как к результатам внутреннего контроля, так и к результатам проверок (государственного надзора):

(1) перечень санкций приведен с точки зрения выявления правовых рисков Оператора как юридического лица. Вопросы юридической ответственности сотрудников Оператора и третьих лиц не рассматриваются;

(2) перечень типовых рекомендаций по устранению несоответствий не является исчерпывающим и достаточным, и Оператор может рассмотреть необходимость применения дополнительных мер и мероприятий по устранению несоответствий;

(3) перечень типовых рекомендаций может быть вариативным (в этих случаях рекомендациям присвоены порядковые номера – 1, 2, 3 и т.д.), то есть возможно применение только части предложенных рекомендаций. Например, контроль, указанный в п.7, может ограничиться только получением согласия субъекта ПДн, а остальные две рекомендации не будут применимы.

2.9.4 Контроли несоответствий требованиям действующего законодательства РФ в области ПДн, соответствующие им меры юридической ответственности, а также рекомендации по устранению несоответствий:

Таблица № 1. Контроли несоответствий.

№	Контроли	Несоответствия	Санкции	Рекомендации
1	ч.2 ст.5 152-ФЗ п.1 ст.86 ТК РФ	Обработка ПДн, несовместимая с целями сбора ПДн.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить цели обработки ПДн в локальном нормативном общедоступном акте.
2	ч.3 ст.5 152-ФЗ	Объединение БД, содержащих ПДн,	ст.13.11 КоАП РФ	Разделить БД, содержащие ПДн, обработка которых

№	Контроли	Несоответствия	Санкции	Рекомендации
		обработка которых осуществляется в целях, несовместимых между собой.	ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	осуществляется в целях, несовместимых между собой.
3	ч.4 ст.5 152-ФЗ	Обрабатываются ПДн, которые не отвечают целям их обработки.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить перечень обрабатываемых ПДн в локальном нормативном общедоступном акте. Прекратить обработку ПДн, не включенных в вышеуказанный перечень.
4	ч.5 ст.5 152-ФЗ п.2 ст.86 ТК РФ	Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить содержание и объем обрабатываемых ПДн в локальном нормативном акте.
5	ч.6 ст.5 152-ФЗ	Не принимаются необходимые меры либо не обеспечивается их принятие по удалению или уточнению неполных или неточных ПДн.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить порядок удаления или уточнения неполных или неточных ПДн в локальном нормативном акте.
6	ч.7 ст.5 152-ФЗ ст.87 ТК РФ	Срок или условие прекращения обработки, а также порядок прекращения обработки ПДн не определены.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить срок или условие прекращения обработки, а также порядок прекращения обработки ПДн в локальном нормативном акте.
7	ч.1 ст.6 152-ФЗ ч.1 ст.152.2 ГК РФ	Обработка ПДн осуществляется без согласия субъекта ПДн или иного законного основания.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151, ч.4 ст.152.2 ГК РФ ст.90 ТК РФ	1. Получить согласие субъекта ПДн в письменной или иной позволяющей подтвердить факт его получения форме. 2. Определить нормы законодательства, позволяющие обрабатывать ПДн без получения согласия субъекта ПДн. 3. Идентифицировать или заново заключить договор, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.
8	ч.3 ст.6 152-ФЗ абз.3 ст.88 ТК РФ	Поручение об обработке ПДн не оформлено (зафиксировано) или оформлено ненадлежащим образом.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Определить и закрепить порядок передачи ПДн третьим лицам в локальном нормативном акте. Указать в типовой форме согласия субъекта на обработку ПДн факты осуществления (или возможного осуществления) передачи ПДн третьим лицам или распространения ПДн. Заключить соглашение между Оператором и обработчиком ПДн, в котором следует определить перечень действий (операций) с ПДн, которые будут совершаться обработчиком ПДн и цели обработки ПДн; установить в

№	Контроли	Несоответствия	Санкции	Рекомендации
				соглашении обязанность обработчика ПДн соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке; указать в соглашении требования к защите обрабатываемых ПДн.
9	ч.2 ст.152.2 ГК РФ	Разглашение сторонами обязательства ставшую известной им при возникновении и (или) исполнении обязательства информацию о частной жизни гражданина, являющегося стороной или третьим лицом в данном обязательстве.	ст.137 УК РФ ч.2 ст.150, ст.151, ч.4 ст.152.2 ГК РФ	1. Прекратить разглашение информации о частной жизни гражданина без его согласия. 2. Если прекращение разглашение информации о частной жизни гражданина невозможно, то следует включить раздел в договор (заключить дополнительное соглашение) о возможности такого разглашения информации о сторонах.
10	ст.7 152-ФЗ абз.2 ст.88 ТК РФ	Раскрытие ПДн третьим лицам и распространение ПДн без согласия субъекта ПДн.	ст.137 УК РФ ст.5.27 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Прекратить раскрытие ПДн третьим лицам и распространение ПДн без согласия субъекта ПДн. 2. Если прекращение раскрытия и/или и распространения ПДн невозможно, то следует определить цель и правовое основание (например, письменное согласие субъекта ПДн) раскрытия и/или распространения ПДн. Также необходимо включить раздел в договор (заключить дополнительное соглашение) с третьим лицом о правомерности передачи ПДн и об обеспечении конфиденциальности передаваемых ПДн.
11	ч.3 ст.152.2 ГК РФ	Неправомерное распространение полученной с нарушением закона информации о частной жизни гражданина, в частности, ее использование при создании произведений науки, литературы и искусства, если такое использование нарушает интересы гражданина.	ст.137 УК РФ ч.2 ст.150, ст.151, ч.4 ст.152.2 ГК РФ	1. Прекратить распространение полученной с нарушением закона информации о частной жизни гражданина. 2. Если распространение полученной с нарушением закона информации о частной жизни гражданина невозможно, то следует определить цель и правовое основание (например, письменное согласие гражданина) для такого распространения.
12	абз.3 ст.88 ТК РФ	Сообщение ПДн сотрудника в коммерческих целях без его письменного согласия.	ст.137 УК РФ ст.5.27 КоАП РФ ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Прекратить сообщение ПДн сотрудника. 2. Если прекращение сообщения ПДн невозможно, то следует определить цель и правовое основание (например, письменное согласие субъекта ПДн) сообщения ПДн.

№	Контроли	Несоответствия	Санкции	Рекомендации
13	ч.1 ст.8 152-ФЗ	Внесение в общедоступные источники ПДн без письменного согласия субъекта ПДн.	ст.137 УК РФ ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151, ч.ч.2 и 3 ст.152.1 ГК РФ ст.90 ТК РФ	1. Прекратить внесение в общедоступные источники ПДн. 2. Если прекращение внесения ПДн невозможно, то следует определить цель и правовое основание (например, письменное согласие субъекта ПДн) внесения ПДн.
14	ч.1 ст.152.1 ГК РФ	Обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) без согласия этого гражданина.	ст.137 УК РФ ч.2 ст.150, ст.151, ч.ч.2 и 3 ст.152.1 ГК РФ	1. Прекратить обнародование и дальнейшее использование изображения гражданина. 2. Если прекращение обнародования и дальнейшего использования изображения гражданина невозможно, то следует определить для них цель и правовое основание (например, письменное согласие гражданина или исключение, указанное в пп.1-3 ч.1 ст.152.1 ГК РФ).
15	ч.1 ст.9 152-ФЗ	Обработка ПДн ведется без наличия оформленного (зафиксированного) соответствующим образом согласия субъекта ПДн, которое дано субъектом свободно, своей волей и в своем интересе. Согласие субъекта ПДн не является конкретным, информированным и сознательным.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Разработать и закрепить в локальном нормативном акте типовую форму письменного согласия субъекта на обработку ПДн. Внедрить типовую форму письменного согласия путем её фактического принятия субъектами ПДн.
16	п.9 ст.86 ТК РФ	Сотрудники отказываются (вынуждены отказаться) от своих прав на сохранение и защиту тайны.	ст.137 УК РФ ст.5.27 КоАП РФ ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Прекратить практику понуждения сотрудников к отказу от своих прав на сохранение и защиту тайны.
17	ч.8 ст.9 152-ФЗ	Получение ПДн от лица, не являющегося субъектом ПДн, без предоставления Оператору подтверждения наличия законных оснований.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Заключить соглашение между Оператором и лицом, не являющимся субъектом ПДн, в котором будет установлена обязанность такого лица предоставлять Оператору доказательства наличия законных оснований для обработки ПДн. 2. Определить нормы законодательства, позволяющие обрабатывать ПДн, полученные Оператором от лица, не являющегося субъектом ПДн.

№	Контроли	Несоответствия	Санкции	Рекомендации
18	ч.2 ст.10 152-ФЗ п.4 ст.86 ТК РФ	Обработка специальных категорий ПДн без письменного согласия субъекта ПДн или иного законного основания.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Получить согласие субъекта ПДн в письменной или иной позволяющей подтвердить факт его получения форме. 2. Определить нормы законодательства, позволяющие обрабатывать ПДн без получения согласия субъекта ПДн. 3. Идентифицировать или заново заключить договор, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.
19	ч.3 ст.10 152-ФЗ	Обработка ПДн о судимости Оператором, не являющимся государственным или муниципальным органом, а также иным лицом, у которого отсутствует прямое указание в законодательстве.	ст.137 УК РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Прекратить обработку ПДн о привлечении субъекта к уголовной ответственности (судимости).
20	п.5 ст.86 ТК РФ	Обработка ПДн сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, если отсутствует прямое указание в законодательстве.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Прекратить обработку ПДн сотрудника. 2. Если прекращение обработки ПДн невозможно, то следует определить цель и правовое основание (норму законодательства) обработки ПДн
21	абз.7 ст.88 ТК РФ	Запрашиваемый объем информации о состоянии здоровья сотрудника превышает объем сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Прекратить обработку ПДн о состоянии здоровья сотрудника.
22	ч.1 ст.11 152-ФЗ	Обработка биометрических ПДн без письменного согласия субъекта ПДн или иного законного основания.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Прекратить обработку биометрических ПДн. 2. Если прекращение обработки биометрических ПДн невозможно, то следует определить цель и правовое основание (например, письменное согласие субъекта ПДн) обработки ПДн.
23	ч.4 ст.12 152-ФЗ	Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, без письменного согласия субъекта ПДн или иного законного основания.	ст.13.11 КоАП РФ ст.13.14 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Указать в локальном нормативном акте сведения, подтверждающие проведение оценки адекватности защиты прав субъектов ПДн на территории иностранного государства. Формализовать в письменной форме согласие субъектов ПДн на трансграничную передачу ПДн на территорию иностранного государства, не обеспечивающего адекватную защиту ПДн.

№	Контроли	Несоответствия	Санкции	Рекомендации
24	ч.1 ст.15 152-ФЗ	Обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации ведется без предварительного согласия субъекта ПДн.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Получить предварительное согласие субъекта ПДн в письменной или иной позволяющей подтвердить факт его получения форме.
25	ч.2 ст.16 152-ФЗ	Решение, порождающее юридические последствия в отношении субъекта ПДн, принимается на основании исключительно автоматизированной обработки его ПДн без письменного согласия субъекта ПДн или иного законного основания.	ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	1. Получить согласие субъекта ПДн в письменной или иной позволяющей подтвердить факт его получения форме. 2. Определить нормы законодательства, позволяющие обрабатывать ПДн без получения согласия субъекта ПДн. 3. Идентифицировать или заново заключить договор, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.
26	п.6 ст.86 ТК РФ	Работодатель при принятии решений, затрагивающих интересы сотрудника, основывается на ПДн сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Не принимать решения, затрагивающие интересы сотрудника, исходя из ПДн сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.
27	ч.3 ст.18 152-ФЗ п.3 ст.86 ТК РФ	Не уведомление субъекта ПДн до начала обработки его ПДн, если ПДн получены не от самого субъекта ПДн.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Включить в типовую форму письменного согласия на обработку ПДн обязательство сотрудников Оператора об уведомлении членов их семей и близких родственников о факте обработки их ПДн Оператором.
28	ч.1 ст.14 152-ФЗ ст.89 ТК РФ	Не обеспечение реализации права субъекта ПДн на доступ к его ПДн, а также права субъекта на уточнение, блокирование, уничтожение его ПДн.	ст.5.27 КоАП РФ ст.5.39 КоАП РФ ст.13.11 КоАП РФ ч.2 ст.150, ст.151 ГК РФ ст.90 ТК РФ	Разработать и закрепить в локальном нормативном акте порядок учета, рассмотрения и реагирования Оператора на запросы субъектов ПДн или их представителей.
29	п.1 ч.1 ст.18.1 152-ФЗ	Не назначено лицо, ответственное за организацию обработки ПДн.	ст.13.11 КоАП РФ	Определить лиц, ответственных за организацию обработки ПДн. Разработать и утвердить соответствующие локальные акты или внести дополнения в имеющиеся локальные акты в сфере организации обработки ПДн.

№	Контроли	Несоответствия	Санкции	Рекомендации
30	п.2 ч.1 ст.18.1 152-ФЗ	Не изданы документы, определяющие политику Оператора в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений	ст.13.11 КоАП РФ ст.19.4.1 КоАП РФ	Актуализировать существующие и разработать отсутствующие локальные акты в сфере организации обработки и обеспечения безопасности ПДн.
31	п.3 ч.1 ст.18.1 152-ФЗ п.7 ст.86 ТК РФ	Не применение правовых, организационных и технических мер по обеспечению безопасности ПДн в соответствии со статьей 19 152-ФЗ.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и ввести в эксплуатацию СЗПДн, включающую в себя применение правовых, организационных и технических мер по обеспечению безопасности ПДн. Более подробно указанные меры рассматриваются в пунктах 38-46 настоящей таблицы.
32	п.4 ч.1 ст.18.1 152-ФЗ	Не осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн законодательству Российской Федерации и локальным актам Оператора.	ст.13.11 КоАП РФ	Определить и закрепить порядок осуществления внутреннего контроля в локальных нормативных актах.
33	п.5 ч.1 ст.18.1 152-ФЗ	Не проведена оценка вреда, который может быть причинен субъектам ПДн в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ.	ст.13.11 КоАП РФ	Определить порядок оценки возможного вреда субъектам ПДн и соотнесения указанного вреда с принимаемыми Оператором мерами. Осуществить оценку возможного вреда.
34	п.8 ст.86 ТК РФ абз.5 ст.88 ТК РФ	Не ознакомление под роспись сотрудников и их представителей с документами работодателя, устанавливающими порядок обработки ПДн сотрудников, а также об их правах и обязанностях в этой области.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ	Разработать и внедрить типовую форму журнала учета ознакомлений с порядком обработки ПДн.
35	п.6 ч.1 ст.18.1 152-ФЗ	Не ознакомление сотрудников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами,	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и внедрить типовую форму журнала учета инструктажей по правилам обработки и защиты ПДн.

№	Контроли	Несоответствия	Санкции	Рекомендации
		определяющими политику Оператора в отношении обработки ПДн, локальными актами по вопросам обработки ПДн, и (или) обучение указанных сотрудников.		
36	ч.2 ст.18.1 152-ФЗ	Не опубликован или иным образом не обеспечен неограниченный доступ к документу, определяющему политику Оператора в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн.	ст.13.11 КоАП РФ	Разработать и разместить в свободном доступе документ, определяющий политику Оператора в отношении обработки и защиты ПДн.
37	абз.6 ст.88 ТК РФ	Доступ к ПДн сотрудников разрешен не только для специально уполномоченных лиц; лица, имеющие доступ к ПДн сотрудников, обладают правом/возможностью получать ПДн сотрудника в большем объеме, чем это им необходимо для выполнения своих функций.	ст.5.27 КоАП РФ ст.13.11 КоАП РФ	Определить и закрепить порядок допуска лиц к обработке ПДн в локальном нормативном акте. Определить перечень лиц, допущенных к обработке ПДн.
38	п.1 ч.2 ст.19 152-ФЗ	Не определены угрозы безопасности ПДн при их обработке в ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Определить актуальные угрозы безопасности ПДн для ИСПДн. Разработать модели угроз на базе методик ФСТЭК России и ФСБ России.
39	п.2 ч.2 ст.19 152-ФЗ	Не применяются организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Создать СЗПДн, включающую в себя организационные и (или) технические меры, определенные для каждой ИСПДн с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ней.
40	п.3 ч.2 ст.19 152-ФЗ	Не применяются прошедшие в установленном порядке процедуру оценки соответствия СЗИ.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	При создании СЗПДн использовать СЗИ, прошедшие в установленном порядке процедуру оценки (в том числе сертифицированные в системах сертификации № РОСС RU.0001.01БИ00 и № РОСС RU.0001.030001).
41	п.4 ч.2 ст.19 152-ФЗ	Не произведена оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Произвести оценку эффективности мер по обеспечению безопасности ПДн для каждой из ИСПДн.
42	п.5 ч.2 ст.19 152-ФЗ	Не осуществляется учет машинных носителей ПДн.	ст.13.11 КоАП РФ ст.13.12	Определить и закрепить порядок учета машинных носителей ПДн в локальном нормативном акте. Разработать и внедрить типовую

№	Контроли	Несоответствия	Санкции	Рекомендации
			КоАП РФ	форму журнала учета материальных носителей, предназначенных для хранения ПДн.
43	п.6 ч.2 ст.19 152-ФЗ	Не осуществляется обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Должны использоваться механизмы регистрации событий, позволяющие обнаруживать факты НСД к ПДн. На случаи НСД к ПДн должны распространяться процедуры контроля и управления инцидентами ИБ Оператора.
44	п.7 ч.2 ст.19 152-ФЗ	Не осуществляется восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Определить и закрепить в локальном нормативном акте порядок восстановления ПДн. Обеспечить фактическое восстановление ПДн.
45	п.8 ч.2 ст.19 152-ФЗ	Не установлены правила доступа к ПДн, обрабатываемым в ИСПДн, а также не обеспечивается регистрация и учет всех действий, совершаемых с ПДн в ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Определить и закрепить в локальном нормативном акте порядок доступа к ПДн, обрабатываемым в ИСПДн. Обеспечить фактическую регистрацию и учет всех действий, совершаемых с ПДн в ИСПДн.
46	п.9 ч.2 ст.19 152-ФЗ	Не осуществляется контроль над принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Определить и закрепить в локальных нормативных актах порядок осуществления контроля над принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.
47	ч.1 ст.22 152-ФЗ	Оператор не уведомил Роскомнадзор о своем намерении осуществлять обработку ПДн до начала обработки ПДн или Оператор не уведомил Роскомнадзор об обработке ПДн.	ст.19.7 КоАП РФ	Сформировать уведомление об обработке ПДн и направить его в Роскомнадзор.
48	ч.6 ст.22 152-ФЗ	Оператор предоставил неполные или недостоверные сведения в Роскомнадзор.	ст.19.7 КоАП РФ	Сформировать информационное письмо о внесении изменений в сведения в реестре Операторов, осуществляющих обработку ПДн, и направить его в Роскомнадзор.
49	ч.7 ст.22 152-ФЗ	Оператор не уведомил Роскомнадзор об изменении сведений, указанных в ч.3 ст.22 152-ФЗ, а также в случае прекращения обработки ПДн.	ст.19.7 КоАП РФ	1. Сформировать информационное письмо о внесении изменений в сведения в реестре Операторов, осуществляющих обработку ПДн, и направить его в Роскомнадзор. 2. Сформировать заявление об исключении сведений об Операторе из реестра Операторов, осуществляющих обработку ПДн, и направить его в Роскомнадзор.
50	п.4 ПП-687	ПДн при их обработке, осуществляемой без использования средств автоматизации, не обособляются от иной	ст.13.11 КоАП РФ	Обеспечить фактическое обособление ПДн при их обработке, осуществляемой без использования средств автоматизации.

№	Контроли	Несоответствия	Санкции	Рекомендации
		информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).		
51	п.5 ПП-687	При фиксации ПДн на материальных носителях допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.	ст.13.11 КоАП РФ	Прекратить фиксацию на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Внести изменения в фактический порядок фиксации ПДн на материальных носителях.
52	п.6 ПП-687	Лица, осуществляющие обработку ПДн без использования средств автоматизации, не проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки.	ст.13.11 КоАП РФ	Определить и закрепить порядок обработки и защиты ПДн, обрабатываемых без использования средств автоматизации, в локальных нормативных актах. Разработать и внедрить типовую форму журнала учета инструктажей по правилам обработки и защиты ПДн.
53	п.7 ПП-687	При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, не соблюдаются обязательные условия.	ст.13.11 КоАП РФ	Разработать и внедрить типовые формы документов с учетом требований п.7 ПП-687.
54	п.8 ПП-687	При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится Оператор, или в иных аналогичных целях, не соблюдаются обязательные условия.	ст.13.11 КоАП РФ	Определить и закрепить порядок обработки и защиты ПДн, обрабатываемых без использования средств автоматизации, в локальных нормативных актах. Разработать и внедрить типовую форму журнала учета ПДн для пропуска субъекта ПДн на территорию Оператора.
55	п.9 ПП-687	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, не приняты меры по обеспечению раздельной обработки ПДн.	ст.13.11 КоАП РФ	1. Обеспечить копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию. 2. Обеспечить уничтожение или блокирование материального носителя ПДн с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.
56	п.10 ПП-687	Уничтожение или обезличивание части ПДн, если это допускается материальным носителем,	ст.13.11 КоАП РФ	Определить и закрепить порядок прекращения обработки ПДн в локальном нормативном акте. Разработать и внедрить типовую

№	Контроли	Несоответствия	Санкции	Рекомендации
		производится способом, не исключающим дальнейшую обработку этих ПДн.		форму акт об уничтожении или обезличивании ПДн субъектов.
57	п.13 ПП-687	В отношении каждой категории ПДн, обрабатываемых без использования средств автоматизации, не определены места хранения ПДн (материальных носителей) и не установлен перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.	ст.13.11 КоАП РФ	Определить и закрепить порядок доступа в помещения, в которых ведется обработка ПДн, в локальном нормативном акте. Разработать и принять «Приказ об утверждении мест хранения материальных носителей ПДн», «Приказ об утверждении перечня структурных подразделений и должностей, допущенных к обработке ПДн».
58	п.14 ПП-687	Не обеспечивается раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.	ст.13.11 КоАП РФ	Обеспечить хранение ПДн (материальных носителей) в различных местах хранения (например, хранить материальные носители в разных шкафах).
59	п.15 ПП-687	При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.	ст.13.11 КоАП РФ	Обеспечить условия хранения ПДн (материальных носителей), обеспечивающие их сохранность и исключающие несанкционированный доступ к ним. Это достигается, в том числе, путем ограничения доступа в места расположения материальных носителей и использования запирающихся шкафов, сейфов и т.д.
60	п.8 ПП-1119	Не установлены уровни защищенности ПДн при обработке ПДн в ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Установить уровни защищенности ПДн при обработке ПДн в ИСПДн. Закрепить факт установления уровней защищенности ПДн в соответствующих актах.
61	пп.«а» п.13 ПП-1119	Не организован режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Режим доступа в помещения, в которых размещены ресурсы ИСПДн, должен исключать возможность неконтролируемого нахождения посторонних лиц. Разработать и утвердить документ, определяющий режим доступа на каждой из площадок ИСПДн.
62	пп.«б» п.13 ПП-1119	При хранении материальных носителей не соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Промаркировать все места хранения ПДн и контролировать доступ к материальным носителям на каждой площадки ИСПДн.
63	пп.«в» п.13 ПП-1119	Руководителем Оператора не утвержден документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн,	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и утвердить документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими

№	Контроли	Несоответствия	Санкции	Рекомендации
		необходим для выполнения ими служебных (трудовых) обязанностей.		служебных (трудовых) обязанностей.
64	п.14 ПП-1119	Не назначено должностное лицо (сотрудник), ответственное за обеспечение безопасности ПДн в ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Определить и назначить должностных лиц, ответственных за обеспечение безопасности ПДн в следующих ИСПДн:
65	п.15 ПП-1119	Доступ к содержанию электронного журнала сообщений возможен не только для должностных лиц (сотрудников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и принять приказ об использовании электронного журнала сообщений, в том числе определяющий порядок доступа к содержанию электронного журнала сообщений.
66	пп.«а» п.16 ПП-1119	Не осуществляется автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника Оператора по доступу к ПДн, содержащимся в ИСПДн.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и принять приказ об использовании электронного журнала безопасности. Обеспечить выполнение автоматической регистрации в электронном журнале безопасности изменений полномочий сотрудника Оператора по доступу к ПДн, содержащимся в ИСПДн.
67	пп.«б» п.16 ПП-1119	Не создано структурное подразделение, ответственное за обеспечение безопасности ПДн в ИСПДн, либо функции по обеспечению такой безопасности не возложены на одно из структурных подразделений.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	Разработать и утвердить документ о структурном подразделении, ответственном за обеспечение безопасности ПДн при их обработке в ИСПДн. Возложить функции по обеспечению безопасности ПДн в ИСПДн на одно из структурных подразделений или создать структурное подразделение, ответственное за обеспечение безопасности ПДн в ИСПДн.
68	п.17 ПП-1119	Контроль за выполнением требований ПП-1119 не организуется и не проводится Оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.	ст.13.11 КоАП РФ ст.13.12 КоАП РФ	1. Определить и закрепить в локальном нормативном акте порядок осуществления контроля над выполнением требований ПП-1119. 2. Для осуществления контроля над выполнением требований ПП-1119 привлечь на договорной основе юридическое лицо, имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3 Порядок организации обработки ПДн

3.1 Основные правила обработки ПДн

3.1.1 Утверждаются решением генерального директора Компании:

(1) перечень обрабатываемых Оператором ПДн;

(2) перечень ИСПДн Оператора.

3.1.2 Цели обработки ПДн определены в п.4.2 «Политики ООО «Витте Про» в отношении организации обработки и обеспечения безопасности персональных данных».

3.1.3 Обработка ПДн включает действия (операции), перечисленные в п.4.4 «Политики организации обработки и обеспечения безопасности персональных данных в ООО «Витте Про», но не ограничивается ими.

3.1.4 Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

3.1.5 Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки.

3.1.6 Не допускается объединение БД, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

3.2 Порядок предоставления доступа сотрудников к ПДн

3.2.1 Доступ к ПДн имеют сотрудники Компании, которые обязаны осуществлять их обработку в связи с исполнением своих должностных обязанностей (служба управления персоналом, бухгалтерия).

3.2.2 Перечень сотрудников Компании, осуществляющих обработку ПДн, определяется Ответственным за обработку персональных данных лицом и утверждается генеральным директором.

3.2.3 Процедура предоставления доступа сотрудника Компании к ПДн предусматривает:

(1) подачу непосредственным руководителем сотрудника служебной записки в адрес Ответственного лица с указанием фамилии, имени, отчества, должности и подразделения сотрудника, действия (действий) по обработке ПДн, в котором будет участвовать сотрудник, описания выполняемых сотрудником функций по обработке ПДн;

(2) ознакомление сотрудника под роспись с Положением, другими локальными

актами Компании по вопросам обработки ПДн, а также локальными актами, устанавливающими процедуры, направленные на выявление нарушений законодательства РФ в области обработки и защиты ПДн и устранение последствий таких нарушений;

(3) информирование сотрудника о категориях обрабатываемых ПДн, об особенностях и правилах осуществления обработки ПДн;

(4) фиксацию в письменной форме обязательства сотрудника, включающего положения:

(4.1) об обеспечении конфиденциальности и безопасности ПДн, непосредственно обрабатываемых сотрудником;

(4.2) о прекращении обработки ПДн, ставших известными в связи с исполнением должностных обязанностей, в случае расторжения с сотрудником трудового договора;

(5) проведение инструктажа и регистрацию Ответственным лицом факта проведения инструктажа в «Журнале учёта проведения инструктажей сотрудников по соблюдению правил обработки и защиты ПДн».

3.2.4 В случае увольнения, перевода на другую должность или изменения должностных обязанностей сотрудника, обрабатывающего ПДн, а также изменении организационно-штатной структуры, непосредственный руководитель сотрудника, обрабатывающего ПДн, уведомляет об этом лицо, ответственное за организацию обработки ПДн, Рабочей группой по указанию Ответственного лица осуществляется пересмотр прав доступа сотрудника к ПДн и при необходимости вносятся соответствующие изменения в Перечень сотрудников, допущенных к обработке ПДн.

3.2.5 При увольнении сотрудника, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, передаются другому сотруднику, имеющему доступ к ПДн по указанию непосредственного руководителя увольняющегося сотрудника.

3.2.6 Лицо, ответственное за организацию обработки ПДн, не реже одного раза в месяц осуществляет проверку/актуализацию Перечня сотрудников, допущенных к обработке ПДн, а также списка пользователей ИСПДн, электронного журнала обращений пользователей ИСПДн на получение ПДн. В случае выявления сотрудников, допущенных к обработке ПДн, которым такой доступ больше не требуется, права доступа такого сотрудника к ПДн незамедлительно отзываются.

3.2.7 Допуск сотрудников к обработке ПДн до прохождения процедуры предоставления доступа запрещается.

3.2.8 Доступ сотрудников к своим ПДн осуществляется в соответствии с положениями 152-ФЗ и трудового законодательства.

3.3 Порядок обработки ПДн, включая сбор, хранение и уточнение ПДн

3.3.1 Сбор ПДн в Компании осуществляется в соответствии с целями обработки ПДн.

3.3.2 Обработка ПДн может осуществляться Компанией в случаях, если:

(1) обработка ПДн осуществляется с согласия субъекта на обработку его ПДн;

(2) обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;

(3) обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве;

(4) обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

(5) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение согласия субъекта ПДн невозможно;

(6) обработка ПДн необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

(7) обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в ст.15 152-ФЗ, при условии обязательного обезличивания ПДн;

(8) осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом либо по его просьбе;

(9) осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

(10) осуществляется обработка специальных категорий ПДн, касающихся состояния здоровья, а также биометрических ПДн в соответствии с согласием субъекта ПДн в письменной форме на обработку своих ПДн, в силу того, что ПДн сделаны общедоступными субъектом ПДн или при наличии иных законных оснований.

3.3.3 Субъекту ПДн сообщается о целях, способах и источниках получения его ПДн, а также о характере подлежащих получению ПДн и возможных последствиях

отказа субъекта дать письменное согласие на их получение.

3.3.4 ПДн субъектов могут храниться на материальных носителях информации.

3.3.5 Порядок хранения ПДн определяется Ответственным лицом, и должен исключать несанкционированный доступ третьих лиц к ПДн.

3.3.6 При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», обеспечивается запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан РФ с использованием БД, находящихся на территории РФ, за исключением случаев, указанных в п.п.2, 3, 4, 8 ч.1 ст.6 152-ФЗ.

3.3.7 Бумажные носители ПДн, обрабатываемых в сходных целях, могут храниться в общих хранилищах. Запрещается хранить совместно на бумажных носителях ПДн, обрабатываемые в несовместимых целях.

3.3.8 Вводимые в эксплуатацию электронные носители ПДн и хранилища бумажных носителей ПДн учитываются Ответственным лицом в «Журнале учёта носителей, предназначенных для хранения ПДн».

3.4 Порядок уничтожения ПДн

3.4.1 Сроки и условия прекращения обработки ПДн закреплены в п.4.3 «Политики организации обработки и обеспечения безопасности персональных данных в ООО «Витте Про».

3.4.2 При невозможности уничтожения ПДн в сроки, определенные 152-ФЗ для случаев, когда невозможно обеспечить правомерность обработки ПДн, при достижении целей обработки ПДн, а также при отзыве субъектом согласия на обработку ПДн, если сохранение ПДн более не требуется для целей обработки ПДн, Компания осуществляет блокирование ПДн и уничтожает ПДн в течение 6 месяцев, если иной срок не установлен законодательством РФ.

3.4.3 Уничтожение ПДн должно производиться способом, исключающим возможность восстановления этих ПДн. Уничтожение носителей ПДн должно производиться комиссией, состав которой определяется Ответственным лицом. Факт уничтожения носителя ПДн подтверждается «Актом об уничтожении ПДн».

3.4.4 Уничтожение ПДн в ИСПДн и машинных (материальных) носителей ПДн осуществляется с помощью штатных средств.

3.4.5 Уничтожение бумажных носителей ПДн осуществляется в установленном Оператором порядке после передачи в архив и (или) истечении сроков хранения.

4 Порядок обеспечения безопасности ПДн при их обработке в ИСПДн

4.1 Возложение ответственности за обеспечение безопасности ПДн

4.1.1 Для каждой из действующих ИСПДн, в отношении которой установлена необходимость обеспечения 1-го уровня защищённости ПДн, генеральным директором Компании формируется или назначается структурное подразделение, ответственное за обеспечение безопасности ПДн при их обработке в ИСПДн. При этом одно структурное подразделение может являться ответственным за обеспечение безопасности ПДн при их обработке в нескольких ИСПДн.

4.1.2 Для каждой из ИСПДн, в отношении которой установлена необходимость обеспечения 2-го или 3-го уровня защищённости ПДн, генеральным директором назначается должностное лицо, ответственное за обеспечение безопасности ПДн при их обработке в данной ИСПДн. При этом одно должностное лицо может являться ответственным за обеспечение безопасности ПДн при их обработке в нескольких ИСПДн.

4.1.3 Компания определяет и внедряет организационные и технические мероприятия, необходимые и достаточные в соответствии с требованиями действующего законодательства РФ для обеспечения безопасности ПДн при их обработке в ИСПДн.

4.2 Основные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн

4.2.1 Компанией самостоятельно или с привлечением внешней организации, обладающей лицензией на деятельность по технической защите конфиденциальной информации, определяется перечень актуальных угроз безопасности ПДн при их обработке в каждой из ИСПДн.

4.2.2 Компанией самостоятельно или с привлечением внешней организации, обладающей лицензией на деятельность по технической защите конфиденциальной информации, определяется необходимый уровень защищённости ПДн при их обработке в каждой из ИСПДн, оператором которой он является.

4.2.3 Компанией самостоятельно или с привлечением организации, обладающей лицензиями на деятельность по технической защите конфиденциальной информации и на деятельность по выполнению работ и оказанию услуг в области шифрования информации, создаётся система защиты ПДн, включающая в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИС.

4.2.4 Компания обеспечивает выполнение следующих основных мероприятий:

(1) организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

(2) обеспечение сохранности носителей ПДн;

(3) актуализация утвержденного генеральным директором документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей;

(4) использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, при этом сертификаты на СЗИ должны быть действительными;

(5) формирование или назначение структурного подразделения, ответственного за обеспечение безопасности ПДн при их обработке в ИСПДн (для ИСПДн, в отношении которых установлена необходимость обеспечения 1-го уровня защищённости);

(6) назначение лица, ответственного за обеспечение безопасности ПДн в ИСПДн (для ИСПДн, в отношении которых установлена необходимость обеспечения 2-го и 3-го уровня защищённости);

(7) ограничение доступа к содержанию электронного журнала сообщений: доступ должен быть возможен исключительно для должностных лиц (сотрудников) Оператора ИСПДн или уполномоченного им лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей (для ИСПДн, в отношении которых установлена необходимость обеспечения 2-го уровня защищённости);

(8) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника Оператора ИСПДн по доступу к ПДн, содержащимся в ИСПДн (для ИСПДн, в отношении которых установлена необходимость обеспечения 1-го уровня защищённости).

4.2.5 Лицо, ответственное за организацию обработки ПДн, получив информацию о факте нарушения действующих законодательных норм по обеспечению безопасности ПДн в ИСПДн, организует проведение служебного расследования для выявления лиц, в результате действий или бездействия которых произошло нарушение законодательных норм по обеспечению безопасности ПДн.

4.2.6 Лицо, ответственное за обеспечение безопасности ПДн в ИСПДн, имеет право:

(1) требовать от обеспечивающих ИБ и применение ИТ сотрудников Компании выполнения следующих действий, предусмотренных законодательством РФ, а также локальными актами, но не ограничиваясь ими:

(1.1) осуществлять регулярное обнаружение уязвимостей и угроз безопасности ПДн;

(1.2) участвовать в определении актуальных угроз безопасности ПДн;

(1.3) проводить работы по проработке технических решений по защите ПДн, внедрению и эксплуатации программных и аппаратных средств защиты, а также инфраструктуры ИСПДн;

(1.4) участвовать в разработке и поддержании в актуальном состоянии организационно-распорядительной документации СЗПДн;

(1.5) участвовать в реализации разрешительной системы доступа к ПДн;

(2) запрашивать и получать от иных сотрудников Компании информацию для исполнения своих обязанностей;

(3) вносить предложения руководству компании:

(2.1) о внесении изменений в технологические процессы, связанные с обработкой ПДн, а также в ИСПДн, если это обусловлено необходимостью обеспечения безопасности ПДн в соответствии с требованиями законодательства РФ;

(2.2) о необходимости проведения организационных и технических мероприятий с целью обеспечения безопасности ПДн в соответствии с требованиями законодательства РФ;

(2.3) о поощрении или привлечении к ответственности сотрудников в связи с исполнением ими обязанностей, связанных с обработкой ПДн;

(2.4) о привлечении организации, обладающей лицензией ФСТЭК России, на осуществление деятельности по технической защите конфиденциальной информации, для разработки частных моделей угроз и нарушителя, а также для проведения организационных и технических мероприятий по обеспечению безопасности ПДн.

4.2.7 Лицо, ответственное за обеспечение безопасности ПДн в ИСПДн, обязано обеспечить:

(1) разработку Модели защиты ПДн при их обработке в ИСПДн;

(2) определение типа актуальных угроз ИБ ПДн для каждой ИСПДн;

(3) определение необходимого уровня защищённости ПДн при их обработке в ИСПДн;

(4) определение требований к созданию СЗПДн для ИСПДн;

(5) выбор СЗИ для СЗПДн в соответствии с П-21;

(6) проектирование СЗПДн;

(7) создание и ввод в эксплуатацию СЗПДн;

(8) учет применяемых для обеспечения безопасности ПДн СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ;

(9) проведение и учет инструктажей лиц, допущенных к работе с СКЗИ, применяемых для обеспечения безопасности ПДн;

(10) контроль выполнения мероприятий, предусмотренных в п.4.2.4 Положения.

5 Лицо, ответственное за организацию обработки ПДн

5.1 Статус лица, ответственного за организацию обработки ПДн

5.1.1 Генеральный директор Компании назначает лицо, ответственное за организацию обработки ПДн, которое при осуществлении своих функций руководствуется Положением, «Политикой организации обработки и обеспечения безопасности персональных данных в ООО «Витте Про», иными локальными актами в сфере организации обработки и обеспечения безопасности ПДн, а также требованиями действующего законодательства РФ о ПДн.

5.1.2 По предложению лица, ответственного за организацию обработки ПДн, формируется рабочая группа, состоящая из сотрудников Оператора. В состав рабочей группы могут входить представители подразделений, в которых обрабатываются ПДн. Руководство рабочей группой осуществляется лицом, ответственным за организацию обработки ПДн.

5.1.3 Решения об инициации Компанией новых процессов обработки ПДн или о внесении изменений в существующие процессы обработки ПДн согласовываются с лицом, ответственным за организацию обработки ПДн.

5.2 Функции лица, ответственного за организацию обработки ПДн

5.2.1 Лицо, ответственное за организацию обработки ПДн в Компании, осуществляет следующие функции:

(1) осуществление внутреннего контроля над соблюдением сотрудниками законодательства РФ о ПДн, в том числе требований к защите ПДн;

(2) подготовка перечня структурных подразделений и должностных лиц, допущенных к обработке ПДн, в том числе в ИСПДн, для выполнения служебных (трудовых) обязанностей;

(3) ознакомление сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику в отношении обработки ПДн, локальными актами по вопросам обработки и защиты ПДн, и обучение

указанных сотрудников;

(4) принятие и обработка обращений и запросов субъектов ПДн или их представителей и (или) осуществление контроля над приемом и обработкой таких обращений и запросов;

(5) оценка соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн;

(6) разработка документов, определяющих политику в отношении обработки ПДн, локальных актов Оператора по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ о ПДн, а также устранение последствий таких нарушений;

(7) проведение мероприятий по внутреннему контролю и (или) аудиту соответствия обработки ПДн требованиям 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политикой в отношении обработки ПДн, локальным актам;

(8) оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ;

(9) установление правил доступа сотрудников к ПДн, обрабатываемым в ИСПДн;

(10) совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Компании, осуществление взаимодействия с Роскомнадзором и иными уполномоченными органами в случаях, предусмотренных законодательством РФ о ПДн;

(11) своевременное формирование и направление в Роскомнадзор уведомления об обработке (о намерении осуществлять обработку) ПДн;

(12) своевременное формирование и направление в Роскомнадзор информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн;

(13) осуществление регулярного мониторинга фактов включения в ежегодный сводный план проведения плановых проверок субъектов предпринимательства на предмет соблюдения обязательных требований в сфере обработки ПДн;

(14) организация работы по получению согласия субъектов ПДн на обработку их ПДн в случаях, предусмотренных законодательством РФ о ПДн;

(15) ведение учета процессов обработки ПДн и перечня ИСПДн, а также поддержание в актуальном состоянии описательной документации для них;

(16) совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов, осуществление экспертизы локальных актов и договоров с третьими лицами на предмет их соответствия требованиям законодательством РФ о ПДн.

5.3 Полномочия лица, ответственного за организацию обработки ПДн

5.3.1 Лицо, ответственное за организацию обработки ПДн в Компании, обладает следующими полномочиями:

(1) требовать от сотрудников выполнения требований локальных актов по вопросам обработки и защиты ПДн, а также законодательства РФ о ПДн;

(2) запрашивать и получать от сотрудников информацию для исполнения своих прав и обязанностей, приведенных в Положении;

(3) вносить предложения руководителю о внесении изменений в процессы обработки ПДн и технологические процессы, связанные с обработкой ПДн в ИСПДн, если это обусловлено необходимостью обеспечения соответствия законодательству РФ о ПДн;

(4) вносить предложения руководителю о поощрении или наложении взысканий на сотрудников Оператора в связи с исполнением ими обязанностей, связанных с обработкой и защитой ПДн;

(5) поручать непосредственное осуществление обязанностей, возложенных Положением на лицо, ответственное за организацию обработки ПДн, сотрудникам и иным лицам, входящим в рабочую группу Ответственного лица – в соответствии с п.5.1.2 Положения.

5.4 Ответственность лица, ответственного за организацию обработки ПДн

5.4.1 Лицо, ответственное за организацию обработки ПДн, несет следующую ответственность:

(1) за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных Положением, в пределах, определенных действующим трудовым законодательством РФ;

(2) за правонарушения, совершенные в процессе осуществления своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством РФ;

(3) за причинение материального ущерба и морального вреда в пределах, определенных действующим трудовым и гражданским законодательством РФ.

6 Порядок взаимодействия с субъектами ПДн или их представителями

6.1 Основные правила взаимодействия с субъектами ПДн

6.1.1 Ответственными сотрудниками Компании за взаимодействие с субъектами ПДн назначаются:

(1) с сотрудниками – уполномоченный сотрудник Оператора, осуществляющий кадровый учет;

(2) с прочими субъектами, обработка которых предусмотрена договорными отношениями субъекта или его представителя – лицо, ответственное за организацию обработки ПДн.

6.1.2 Субъекты, ПДн которых обрабатываются в Компании, имеют право:

(1) получать доступ к своим ПДн;

(2) требовать от Компании уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

(3) получать следующую информацию:

(3.1) подтверждение факта обработки ПДн;

(3.2) правовые основания обработки ПДн;

(3.3) цели и применяемые способы обработки ПДн;

(3.4) наименование и место нахождения, сведения о лицах (за исключением сотрудников), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора или на основании федерального закона;

(3.5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

(3.6) сроки обработки ПДн, в том числе сроки их хранения;

(3.7) порядок осуществления субъектом ПДн своих прав, предусмотренных 152-ФЗ;

(3.8) информацию об осуществленной, осуществляемой или о планируемой к осуществлению трансграничной ПДн;

(3.9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработка поручена или будет поручена такому лицу.

(4) возражать относительно принятия на основании исключительно

автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъектов ПДн или иным образом затрагивающих их права и законные интересы;

(5) отозвать согласие на обработку ПДн;

(6) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействия Компании при обработке и защите его ПДн.

6.1.3 Субъекты, ПДн которых обрабатываются, обязаны предоставлять достоверные сведения о себе и своевременно информировать об изменении своих ПДн. Компания имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися документами.

6.1.4 Согласие на обработку ПДн Компанией дается субъектом или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Предпочтительной формой получения согласия является письменная форма.

6.1.5 В случае отзыва субъектом согласия на обработку своих ПДн Компания вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии одного или нескольких условий, указанных в пп.2-10 п.3.3.2 Положения.

6.1.6 Выдача сотрудникам Компании документов, связанных с их трудовой деятельностью (копий приказов о приеме на работу, переводах на другую работу, увольнении с работы; выписок из трудовой книжки, справок о месте работы, заработной плате, периоде работы в организации и др.), производится соответствующим уполномоченным сотрудником, осуществляющим кадровый учет, в порядке, установленном законодательством РФ. Справки о заработной плате, о месте работы и о периоде работы выдаются сотруднику под подпись в соответствующем журнале учета выдачи справок.

6.1.7 Устные запросы субъекта ПДн или его представителя фиксируются в «Журнале учета обращений субъектов ПДн или их представителей» (Приложение 4) или в иных документах, обеспечивающих надлежащую фиксацию запросов субъекта ПДн или его представителя.

6.1.8 В случае поступления запроса от субъекта ПДн или его представителя в письменной форме о предоставлении сведений, указанных в пп.3 п.6.1.2 Положения, лицо, ответственное за организацию обработки ПДн, подготавливает согласно запросу субъекта или его представителя необходимый ответ в письменной форме. В случае требования предоставления иных, непредусмотренных законодательством сведений, лицо, ответственное за организацию обработки ПДн, подготавливает мотивированный ответ в письменной форме, содержащий ссылку на положение ч.8 ст.14 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не

превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

6.1.9 Документы, содержащие ПДн субъекта, могут быть отправлены через организацию федеральной почтовой связи, курьерской почтой или нарочным. При этом должны быть предприняты разумные и достаточные меры для обеспечения конфиденциальности ПДн.

6.1.10 Лицо, ответственное за организацию обработки ПДн, обязано организовать текущее хранение нижеуказанных документов в течение пяти лет, а по истечении указанного срока – обеспечить передачу следующих документов на архивное хранение:

(1) запросы субъекта ПДн или его представителя;

(2) копии документов, являющихся основанием для уточнения или отказа в уточнении обрабатываемых ПДн;

(3) копии документов, являющихся основанием для прекращения неправомерной обработки ПДн или отказа в прекращении обработки ПДн;

(4) копии документов, являющихся основанием для отказа в прекращении обработки ПДн;

(5) уведомления субъекта ПДн или его представителя об уточнении или об отказе уточнения обрабатываемых ПДн;

(6) уведомления субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн или отказе в прекращении обработки ПДн;

(7) уведомления субъекта ПДн или его представителя о прекращении обработки ПДн или отказе в прекращении обработки ПДн;

(8) иные документы и копии иных документов, непосредственно связанные с выполнением Оператором своих обязанностей по рассмотрению запросов субъекта ПДн или его представителя.

6.2 Обработка запросов об уточнении неполных, устаревших, неточных ПДн

6.2.1 В случае запроса субъекта ПДн или его представителя об уточнении Оператором (или лицом, действующим по поручению Оператора) обработки неполных, устаревших, неточных ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) зафиксировать наличие запроса субъекта ПДн или его представителя об уточнении обработки неполных, устаревших, неточных ПДн в «Журнале учета обращений субъектов персональных данных или их представителей» или в иных документах, обеспечивающих надлежащую фиксацию запросов субъекта ПДн

или его представителя;

(2) осуществить блокирование указанных ПДн с момента получения запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;

(3) осуществить проверку фактов, изложенных в запросе, и подтверждающих факты документов, предоставляемых субъектом ПДн или его представителем. По результатам проверки должно быть получено подтверждение или не подтверждение фактов, изложенных в запросе.

6.2.2 В случае подтверждения фактов, изложенных в запросе, лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) произвести/обеспечить уточнение указанных ПДн на основании представленных сведений в течение семи рабочих дней со дня представления таких сведений;

(2) осуществить снятие блокирования указанных ПДн;

(3) в письменной форме уведомить субъекта ПДн или его представителя об устранении допущенных нарушений.

6.2.3 В случае не подтверждения фактов, изложенных в запросе, лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) осуществить снятие блокирования указанных ПДн;

(2) в письменной форме уведомить субъекта ПДн или его представителя об отказе в уточнении ПДн.

6.3 Обработка запросов о прекращении неправомерной обработки ПДн

6.3.1 В случае запроса субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) зафиксировать наличие запроса субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн в «Журнале учета обращений субъектов персональных данных или их представителей» или в иных документах, обеспечивающих надлежащую фиксацию запросов субъекта ПДн или его представителя;

(2) осуществить блокирование указанных ПДн с момента получения запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;

(3) осуществить проверку фактов, изложенных в запросе, и подтверждающих

факты документов, предоставляемых субъектом ПДн или его представителем. По результатам проверки должно быть получено подтверждение или не подтверждение фактов, изложенных в запросе.

6.3.2 В случае подтверждения факта неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) произвести/обеспечить прекращение неправомерной обработки ПДн в срок, не превышающий трех рабочих дней со дня выявления неправомерной обработки ПДн;

(2) если обеспечить правомерность обработки ПДн невозможно, то уничтожить такие ПДн или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней со дня выявления неправомерной обработки ПДн;

(3) в письменной форме уведомить субъекта ПДн или его представителя о прекращении неправомерной обработки ПДн.

6.3.3 В случае не подтверждения факта неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) осуществить снятие блокирования указанных ПДн;

(2) в письменной форме уведомить субъекта ПДн или его представителя об отказе в прекращении обработки ПДн.

6.4 Обработка отзывов согласий на обработку ПДн

6.4.1 В случае отзыва субъектом ПДн или его представителем согласия на обработку его ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны зафиксировать наличие отзыва субъектом ПДн или его представителем согласия на обработку ПДн в «Журнале учета обращений субъектов персональных данных или их представителей» или в иных документах, обеспечивающих надлежащую фиксацию запросов субъекта ПДн или его представителя.

6.4.2 Если обработка ПДн осуществляется при выполнении условия, указанного в пп.1 п.3.3.2 Положения, лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) уведомить субъекта ПДн или его представителя о последствиях отзыва им согласия;

(2) организовать уничтожение ПДн;

(3) в письменной форме уведомить субъекта ПДн или его представителя о

прекращении обработки ПДн субъекта.

6.4.3 Если обработка ПДн осуществляется при выполнении условий, указанных в пп.2-10 п.3.3.2 Положения, лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны в письменной форме (содержащий ссылку на положения ч.2 ст.9 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа) уведомить субъекта ПДн или его представителя об отказе в прекращении обработки ПДн.

6.5 Предоставление ПДн субъектов их представителям, членам их семей и родственникам

6.5.1 Представителю субъекта (в том числе адвокату) передача ПДн производится в порядке, установленном действующим законодательством РФ. Информация передается при наличии одного из документов:

(1) нотариально удостоверенной доверенности представителя субъекта ПДн;

(2) письменного заявления субъекта ПДн, написанного в присутствии лица, ответственного за организацию обработки ПДн, или иного уполномоченного сотрудника. Если заявление написано субъектом ПДн не в присутствии указанных лиц, то оно должно быть нотариально заверено.

6.5.2 ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством РФ.

7 Порядок обмена информацией, содержащей ПДн, с третьим лицами и неопределенным кругом лиц

7.1 Получение ПДн

7.1.1 ПДн могут быть получены от лица, не являющегося субъектом ПДн, при условии предоставления подтверждения выполнения условий, указанных в п.3.3.2 Положения.

7.1.2 В случае невозможности представления подтверждения, указанного в п. 7.1.1, Оператор осуществляет уведомление субъекта ПДн в письменной форме об обработке его персональных данных.

7.2 Раскрытие ПДн

7.2.1 Раскрытие ПДн неопределенному кругу лиц осуществляется с согласия субъекта ПДн в письменной форме.

7.2.2 Раскрытие ПДн определенному лицу или определенному кругу лиц осуществляется с согласия субъекта ПДн в письменной форме, которое оформляется по установленной форме и должно включать в себя:

(1) фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

(2) наименование и адрес организации (третьего лица), получающей ПДн субъекта;

(3) цель передачи ПДн;

(4) перечень ПДн, на передачу которых дает согласие субъект;

(5) срок, в течение которого действует согласие, а также порядок его отзыва;

(6) подпись субъекта ПДн.

7.3 Передача ПДн

7.3.1 Согласия субъекта на передачу его ПДн третьим лицам не требуется:

(1) в целях предупреждения угрозы жизни и здоровью субъекта ПДн;

(2) когда согласие субъекта на обработку (в том числе передачу) его ПДн третьими лицами получено от него в письменном виде при заключении договора с Компанией;

(3) когда третьи лица оказывают услуги Компании на основании заключенных договоров, а передача ПДн необходима для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект ПДн;

(4) в иных случаях, установленных действующим законодательством РФ.

7.3.2 ПДн субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта, за исключением случаев, когда передача ПДн субъекта без его согласия допускается действующим законодательством РФ либо договором, регламентирующим правоотношения с субъектом.

7.3.3 Ответы на запросы третьих лиц (в том числе, юридических лиц) в пределах их компетенции и предоставленных полномочий даются в письменной форме, на бланке организации и в том объеме, который позволяет не разглашать излишний объем ПДн о субъектах.

7.3.4 Сотрудники, передающие документы (или иные материальные носители информации) с ПДн субъектов третьим лицам, должны передавать их либо с составлением двустороннего акта приема-передачи документов (иных материальных

носителей информации), содержащих ПДн субъектов, либо иным способом, позволяющим подтвердить факт и дату передачи документов (или иных материальных носителей информации), содержащих ПДн. При использовании любого из указанных способов должны выполняться следующие условия:

(1) уведомление лица, получающего данные документы об обязанности использования полученных ПДн лишь в целях, для которых они сообщены;

(2) предупреждение об ответственности за противоправную обработку ПДн в соответствии с действующим законодательством РФ.

7.3.5 Передача документов (иных материальных носителей информации), содержащих ПДн субъектов, осуществляется при наличии у лица, уполномоченного на их получение одного из наборов документов, указанных в п.7.3.6 и п.7.3.7 Положения.

7.3.6 Первый набор документов:

(1) договор, стороной или выгодоприобретателем которого является Оператор;

(2) соглашение о соблюдении конфиденциальности информации либо наличие в договоре с третьим лицом пунктов о соблюдении конфиденциальности информации, в том числе, предусматривающих обеспечение конфиденциальности ПДн субъекта;

7.3.7 Второй набор документов:

(1) письмо-запрос от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей ПДн субъекта, её перечень, цель использования, фамилию, имя, отчество и должность лица, которому поручается получить данную информацию;

(2) соглашение о соблюдении конфиденциальности информации, в том числе, предусматривающее обеспечение конфиденциальности ПДн. Наличие подобного соглашения является факультативным, так как могут отсутствовать как юридические основания для заключения соглашения, так и фактическая возможность для его заключения.

7.4 Трансграничная передача ПДн

7.4.1 До начала осуществления трансграничной передачи ПДн необходимо убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн. Адекватная защита прав субъектов ПДн обеспечивается:

(1) иностранными государствами, являющимися сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн;

(2) иностранными государствами, включенными в перечень иностранных

государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и обеспечивающих адекватную защиту прав субъектов ПДн (утверждается Роскомнадзором).

7.4.2 Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться:

(1) при наличии согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;

(2) в случаях, предусмотренных международными договорами РФ;

(3) в случаях, предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя РФ, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

(4) при исполнении договора, стороной которого является субъект ПДн;

(5) для защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

8 Порядок взаимодействия с уполномоченными органами

8.1 Обязанности лица, ответственного за организацию обработки ПДн, при взаимодействии с уполномоченными органами

8.1.1 Ответственность за взаимодействие с уполномоченными органами, осуществляющими мероприятия по контролю над выполнением Компанией требований к обеспечению надлежащей организации обработки и обеспечению безопасности ПДн, в том числе в ИСПДн, несет лицо, ответственное за организацию обработки ПДн.

8.1.2 Лицо, ответственное за организацию обработки ПДн, совместно с представителем структурного подразделения Компании, ответственным за обеспечение соблюдения законности и юридическую защиту интересов Компании, предоставляет уполномоченному органу запрашиваемую им при проведении проверок информацию.

8.1.3 Лицо, ответственное за организацию обработки ПДн, регистрирует сведения о проведении проверки уполномоченными органами в соответствующем журнале учета проверок, проводимых органами государственного контроля (надзора), органами муниципального контроля.

8.1.4 Лицо, ответственное за организацию обработки ПДн, обязано организовать текущее хранение нижеуказанных документов в течение пяти лет, а по истечении указанного срока – обеспечить передачу следующих документов на архивное хранение:

(1) запросы и требования уполномоченных органов;

(2) ответы на запросы и требования уполномоченных органов;

(3) иные документы и копии иных документов, непосредственно связанные с выполнением обязанностей по рассмотрению запросов и требований уполномоченных органов.

8.2 Виды предусмотренных законодательством проверок

8.2.1 Роскомнадзор проводит проверки:

(1) плановые проверки;

(2) внеплановые проверки.

8.2.2 ФСТЭК России проводит следующие проверки:

(1) лицензионный контроль над соблюдением лицензиатом лицензионных требований и условий;

(2) по обращению Роскомнадзора (п. 5.1 ч.3 ст.23 152-ФЗ);

(3) внеплановые проверки по контролю нарушений обязательных требований (ст.10 294-ФЗ).

8.2.3 ФСБ России проводит следующие проверки:

(1) контроль над соблюдением правил пользования СЗКИ;

(2) лицензионный контроль за соблюдением лицензиатом лицензионных требований и условий;

(3) по обращению Роскомнадзора (п. 5.1 ч.3 ст.23 152-ФЗ);

(4) внеплановые проверки по контролю нарушений обязательных требований (ст.10 294-ФЗ).

8.3 Взаимодействие с Роскомнадзором

8.3.1 Роскомнадзор имеет право (ст.23 152-ФЗ):

(1) запрашивать у операторов (физических или юридических лиц) информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

(2) осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн, или привлекать для осуществления такой проверки иные

государственные органы в пределах их полномочий;

(3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

(4) принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований 152-ФЗ;

(5) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов ПДн в суде;

(6) направлять в ФСБ России и в ФСТЭК России применительно к сфере их деятельности, сведения, указанные в п.7 ч.3 ст.22 152-ФЗ;

(7) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством РФ порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу ПДн третьим лицам без согласия в письменной форме субъекта ПДн;

(8) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;

(9) привлекать к административной ответственности лиц, виновных в нарушении требований 152-ФЗ.

8.3.2 При получении запроса на предоставление информации лицо, ответственное за организацию обработки ПДн, проверяет законность такого запроса, после чего предоставляет запрашиваемую информацию в Роскомнадзор.

8.3.3 В случае получения требования Роскомнадзора об уточнении обрабатываемых неполных, устаревших, неточных ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) зафиксировать наличие требования Роскомнадзора об уточнении обработки неполных, устаревших, неточных ПДн;

(2) осуществить блокирование указанных ПДн с момента получения требования на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;

(3) осуществить проверку фактов, изложенных в требовании – по результатам проверки может быть получено подтверждение или не подтверждение факта

неточности ПДн.

8.3.4 В случае подтверждения факта неточности ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник Компании обязаны:

(1) произвести/обеспечить уточнение указанных ПДн на основании представленных сведений в течение семи рабочих дней со дня представления таких сведений;

(2) осуществить снятие блокирования указанных ПДн;

(3) в письменной форме уведомить Роскомнадзор, а также субъекта ПДн или его представителя об устранении допущенных нарушений.

8.3.5 В случае не подтверждения факта неточности ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник Компании обязаны:

(1) осуществить снятие блокирования указанных ПДн;

(2) подготовить и согласовать с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов, ответ в письменной форме о неправомерности требования, и направить его в Роскомнадзор;

(3) совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Компании, подготовить предложение об обжаловании требования в порядке, установленном действующим законодательством РФ.

8.3.6 В случае получения требования Роскомнадзора о прекращении неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник Компании обязаны:

(1) зафиксировать наличие требования Роскомнадзора о прекращении неправомерной обработки ПДн;

(2) осуществить блокирование указанных ПДн с момента получения требования на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц;

(3) осуществить проверку фактов, изложенных в требовании – по результатам проверки может быть получено подтверждение или не подтверждение факта неправомерной обработки ПДн.

8.3.7 В случае подтверждения факта неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) произвести/обеспечить прекращение неправомерной обработки ПДн в срок,

не превышающий трех рабочих дней со дня выявления неправомерной обработки ПДн;

(2) если обеспечить правомерность обработки ПДн невозможно - уничтожить такие ПДн или обеспечить их уничтожение в срок, не превышающий десяти рабочих дней со дня выявления неправомерной обработки ПДн;

(3) в письменной форме уведомить Роскомнадзор, а также субъекта ПДн или его представителя об устранении допущенных нарушений.

8.3.8 В случае не подтверждения факта неправомерной обработки ПДн лицо, ответственное за организацию обработки ПДн, или иной уполномоченный сотрудник обязаны:

(1) осуществить снятие блокирования указанных ПДн;

(2) подготовить и согласовать с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов, ответ в письменной форме о неправомерности требования, и направить его в Роскомнадзор.

(3) совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов, подготовить предложение об обжаловании требования в порядке, установленном действующим законодательством РФ.

8.3.9 При получении иных запросов, выходящих за рамки полномочий Роскомнадзора, лицо, ответственное за организацию обработки ПДн, должно подготовить и согласовать с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Компании, ответ в письменной форме о неправомерности требований, и направить его Роскомнадзор.

8.3.10 При включении Компании в план проверок Роскомнадзора лицо, ответственное за организацию обработки ПДн, незамедлительно уведомляет о предстоящей плановой проверке генерального директора Компании и всех лиц, допущенных к обработке ПДн Оператором, проводит внутреннюю проверку защищенности ПДн (согласно плану и методике проведения внутренних проверок).

8.3.11 При получении уведомления от Роскомнадзора о плановой проверке лицо, ответственное за организацию обработки ПДн:

(1) незамедлительно уведомляет генерального директора Компании и всех лиц, допущенных к обработке ПДн Оператором, о предстоящей проверке;

(2) проводит внутреннюю проверку защищенности ПДн (согласно правилам проведения внутренних проверок).

8.3.12 При получении уведомления от Роскомнадзора о внеплановой проверке лицо, ответственное за организацию обработки ПДн:

(1) запрашивает у должностного лица Роскомнадзора основания для проведения внеплановой проверки;

(2) незамедлительно уведомляет генерального директора Компании и всех лиц, допущенных к обработке ПДн Оператором, о предстоящей проверке;

(3) проводит внутреннюю проверку защищенности ПДн (согласно плана и методике проведения внутренних проверок).

8.3.13 В процессе проведения плановой или внеплановой проверки лицо, ответственное за организацию обработки ПДн:

(1) предоставляет должностным лицам Роскомнадзора информацию, необходимую для реализации проверок;

(2) контролирует соответствие процесса организации (проведения) проверки требованиям действующего законодательства РФ;

(3) регистрирует сведения о проведении проверки в журнале учета проверок, проводимых органами государственного контроля (надзора), органами муниципального контроля.

8.3.14 В случае выездной проверки Роскомнадзора лицо, ответственное за организацию обработки ПДн, должно ознакомиться:

(1) со служебными удостоверениями проверяющих;

(2) с копиями распоряжения или приказа[1] о назначении проверки (под роспись);

(3) с Административным регламентом проведения проверки;

(4) с полномочиями проверяющих, а также с целями, задачами, основаниями проведения проверки, составом экспертов, со сроками и с условиями ее проведения;

(5) с Актом проверки до его подписания (по результатам проверки).

8.3.15 В случае совершения должностными лицами Роскомнадзора при проведении проверки незаконных действий (в том числе нарушающих Административный регламент проверки) или выходящих за рамки их должностных обязанностей, лицо, ответственное за организацию обработки ПДн, совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности

[1] Форма приказа утверждена приказом Министерства экономического развития Российской Федерации от 30.04.2009 № 141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». Проверка должна проводиться проверяющими, которые указаны в приказе.

и юридическую защиту интересов Компании, готовит предложение об обжаловании действий (бездействий) и решения должностных лиц Роскомнадзора в порядке, установленном Административным регламентом проверки и действующим законодательством РФ.

8.4 Взаимодействие с ФСТЭК России, ФСБ России и иными уполномоченными органами

8.4.1 При получении запроса от ФСТЭК России или ФСБ России на предоставление информации лицо, ответственное за организацию обработки ПДн:

(1) проверяет законность такого запроса;

(2) информирует генерального директора Компании, после чего предоставляет запрашиваемую информацию в ФСТЭК России или в ФСБ России.

8.4.2 При получении иных запросов, выходящих за рамки полномочий ФСТЭК России или ФСБ России лицо, ответственное за организацию обработки ПДн, должно подготовить и согласовать с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Компании, письменный ответ о незаконности предъявляемых требований.

8.4.3 При включении Компании в план проверок ФСТЭК России или ФСБ России лицо, ответственное за организацию обработки ПДн, незамедлительно уведомляет о предстоящей плановой проверке генерального директора Компании и всех лиц, допущенных к обработке ПДн, проводит внутреннюю проверку защищенности ПДн (согласно плану и методике проведения внутренних проверок). В процессе проведения проверки ФСТЭК России или ФСБ России лицо, ответственное за организацию обработки ПДн:

(1) предоставляет должностным лицам ФСТЭК России или ФСБ России информацию, необходимую для реализации проверок;

(2) регистрирует сведения о проведении проверки в журнале учета проверок, проводимых органами государственного контроля (надзора), органами муниципального контроля.

8.4.4 В случае незаконных или выходящих за рамки должностных обязанностей действий должностных лиц ФСТЭК России или ФСБ России при проведении проверки лицо, ответственное за организацию обработки ПДн, совместно с представителем структурного подразделения, ответственного за обеспечение соблюдения законности и юридическую защиту интересов Компании, готовит предложение об обжаловании действий (бездействий) и решения должностных лиц ФСТЭК России или ФСБ России в порядке, установленным действующим законодательством РФ.

8.4.5 Взаимодействие с иными уполномоченными органами организуется в порядке, установленном действующим законодательством РФ.

9 Порядок обработки и защиты ПДн, обрабатываемых без использования средств автоматизации

9.1 Обработка ПДн без использования средств автоматизации

9.1.1 Обработка ПДн без использования средств автоматизации (далее – неавтоматизированная обработка ПДн) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, БД) на электронных носителях информации.

9.1.2 При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

9.1.3 При неавтоматизированной обработке ПДн на бумажных носителях:

(1) не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы;

(2) ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

(3) документы, содержащие ПДн, формируются в дела в зависимости от цели обработки ПДн;

(4) дела с документами, содержащими ПДн, должны иметь внутренние описи документов с указанием цели обработки и категории ПДн.

9.1.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовые формы), должны соблюдаться следующие условия:

(1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес оператора, 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;

(2) типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, – при необходимости получения письменного согласия на обработку ПДн;

(3) 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;

(4) типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

9.1.5 Неавтоматизированная обработка ПДн в электронном виде осуществляется на внешних электронных носителях информации.

9.1.6 При отсутствии технологической возможности осуществления неавтоматизированной обработки ПДн в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных СЗИ), исключающие возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

9.1.7 Электронные носители информации, содержащие ПДн, учитываются в «Журнале учета носителей, предназначенных для хранения ПДн» (Приложение 3).

9.1.8 К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории ПДн.

9.1.9 При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном электронном носителе, если электронный 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:

(1) 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;

(2) 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.

9.1.10 Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

9.1.11 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).

9.2 Меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации

9.2.1 Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

9.2.2 Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

9.2.3 При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

10 Порядок обезличивания ПДн

10.1 Цели и условия обезличивания ПДн

10.1.1 Обезличивание ПДн осуществляется в целях:

(1) защиты ПДн от несанкционированного использования;

(2) прекращения обработки ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей;

(3) обработки ПДн в статистических или иных исследовательских целях.

10.1.2 Обезличивание ПДн осуществляется в условиях защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

10.2 Требования к методам обезличивания ПДн

10.2.1 Требования к методам обезличивания ПДн подразделяются на:

(1) требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;

(2) требования к свойствам, которыми должен обладать метод обезличивания.

10.2.2 К требованиям к свойствам получаемых обезличенных данных относятся:

(1) сохранение полноты (состав обезличенных данных должен полностью

соответствовать составу обезличиваемых ПДн);

(2) сохранение структурированности обезличиваемых ПДн;

(3) сохранение семантической целостности обезличиваемых ПДн;

(4) анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания как, например, k-anonymity).

10.2.3 К требованиям к свойствам метода обезличивания относятся:

(1) обратимость (возможность проведения деобезличивания);

(2) возможность обеспечения заданного уровня анонимности;

(3) увеличение стойкости при увеличении объема обезличиваемых ПДн.

10.3 Методы обезличивания ПДн

10.3.1 Методы обезличивания должны обеспечивать требуемые свойства обезличенных ПДн, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки ПДн.

10.3.2 Методы обезличивания ПДн при условии дальнейшей работы с обезличенными данными:

(1) метод введения идентификаторов (замена части сведений (значений ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

(2) метод изменения состава или семантики (изменение состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления части сведений);

(3) метод декомпозиции (разбиение множества (массива) ПДн на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

(4) метод перемешивания (перестановка отдельных записей, а так же групп записей в массиве ПДн).

10.3.3 Методом обезличивания ПДн в случае достижения целей обработки ПДн или в случае утраты необходимости в достижении этих целей является изменение состава или семантики обрабатываемых сведений.

10.4 Порядок обезличивания ПДн и работы с обезличенными данными

10.4.1 Лицо, ответственное за организацию обработки ПДн, готовит предложения по обезличиванию ПДн, включающие обоснование такой необходимости и определение метода(ов) обезличивания.

10.4.2 Генеральный директор Компании, рассмотрев предложения, принимает решение о необходимости обезличивания ПДн и назначает лицо, ответственное за проведение мероприятий по обезличиванию обрабатываемых ПДн.

10.4.3 Сотрудники, осуществляющие эксплуатацию ИСПДн и (или) осуществляющие обработку ПДн без использования средств автоматизации, производят непосредственное обезличивание ПДн в ИСПДн и на бумажных носителях выбранным(ми) методом(ами).

10.4.4 Работа с обезличенными данными осуществляется с использованием и без использования средств автоматизации.

10.4.5 При работе с обезличенными данными с использованием средств автоматизации и без использования средств автоматизации необходимо соблюдение общих правил обеспечения безопасности обработки информации, установленных локальными актами.

11 Порядок доступа сотрудников в помещения, в которых ведется обработка ПДн

11.1 Доступ в помещения, где осуществляется обработка ПДн

11.1.1 Обеспечение безопасности ПДн от уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн достигается, в том числе, установлением правил доступа в помещения, в которых ведется обработка ПДн, как с использованием средств автоматизации, так и без использования средств автоматизации.

11.1.2 Размещение ИСПДн осуществляется в охраняемых помещениях. Для помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ПДн и СЗИ, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

11.1.3 При хранении материальных носителей ПДн в помещениях должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

11.1.4 В помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, допускаются только сотрудники Оператора, уполномоченные осуществлять обработку ПДн.

11.1.5 Ответственными за организацию доступа в помещения являются начальники структурных подразделений или должностные лица, использующие данные помещения.

11.1.6 Внутренний контроль над соблюдением порядка доступа в помещения, проводится лицом, ответственным за организацию обработки ПДн.

11.1.7 Нахождение лиц, не уполномоченных осуществлять обработку ПДн, в помещениях возможно только в сопровождении сотрудников вышеуказанных структурных подразделений или должностных лиц на время, ограниченное служебной необходимостью.

11.1.8 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения посторонних лиц, о случившемся должно быть немедленно сообщено лицу, ответственному за организацию доступа в помещение.

11.1.9 В целях обеспечения соблюдения требований к ограничению доступа в помещения обеспечивается:

(1) использование помещений строго по назначению;

(2) наличие на входах в помещения дверей, оборудованных запорными устройствами;

(3) содержание дверей помещений в нерабочее время в состоянии, закрытом на запорное устройство;

(4) содержание окон в помещениях в нерабочее время в закрытом состоянии.

11.2 Доступ в помещения, где размещены СКЗИ и носители информации СКЗИ

11.2.1 Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

11.2.2 Помещения должны иметь прочные входные двери с запорными устройствами, гарантирующими постоянное надёжное запирание помещений в рабочее и в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц в помещения, необходимо оборудовать металлическими решётками или ставнями, охранной сигнализацией и другими средствами, препятствующими неконтролируемому проникновению в помещения.

11.2.3 Размещение, специальное оборудование, охрана и организация режима доступа в помещения должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

11.2.4 Для предотвращения просмотра извне помещений их окна должны быть защищены жалюзи или плотными занавесками.

11.2.5 Помещения должны быть оснащены охранной сигнализацией. Исправность

сигнализации необходимо периодически проверять.

11.2.6 Для хранения носителей ключевой, аутентифицирующей и парольной информации СКЗИ должно быть предусмотрено необходимое число надёжных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

11.2.7 По окончании рабочего дня помещение и установленные в нем хранилища должны быть закрыты и опечатаны. Помещения и хранилища, вместо опечатывания, могут быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

11.2.8 При утрате ключа от хранилища или от входной двери в помещение запорное устройство необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если запорное устройство от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения носителей ключевой, аутентифицирующей и парольной информации СКЗИ в хранилище, от которого утрачен ключ, устанавливает лицо, ответственное за обеспечение безопасности ПДн при их обработке в ИСПДн.

11.2.9 В обычных условиях помещения и находящиеся в них хранилища могут быть вскрыты только пользователями СКЗИ или лицом, ответственным за обеспечение безопасности ПДн при их обработке в ИСПДн.

11.2.10 В условиях чрезвычайных ситуаций в нерабочее время вскрытие помещений осуществляется комиссией в составе не менее двух человек (как то, сотрудники Оператора, сотрудники охраны здания, представители арендодателя и иные уполномоченные лица), с составлением акта о вскрытии.

11.2.11 В акте о вскрытии помещений необходимо указать:

(1) фамилии, имена, отчества должностных лиц, принимавших участие во вскрытии помещения;

(2) причины вскрытия помещения;

(3) дату и время вскрытия помещения;

(4) кто был допущен (должность и фамилия) в помещение;

(5) как осуществлялась охрана вскрытого помещения в этот период;

(6) какое имущество (включая СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ), в каком количестве, куда эвакуировано из вскрытого помещения и как осуществлялась его охрана;

(7) кто из должностных лиц и когда был информирован по указанному факту происшествия;

(8) другие сведения.

11.2.12 Акт о вскрытии помещений подписывается должностными лицами, вскрывшими данные помещения.

11.2.13 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено лицу, ответственному за обеспечение безопасности ПДн при их обработке в ИСПДн, которое должно оценить возможность компрометации хранящихся носителей ключевой, аутентифицирующей, парольной информации СКЗИ и иной информации, составить акт и принять, при необходимости, меры к локализации последствий компрометации указанной информации и к замене скомпрометированных криптоключей.

11.2.14 Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

11.2.15 На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в хранилища. В противном случае по согласованию с лицом, ответственным за обеспечение безопасности ПДн при их обработке в ИСПДн, необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

12 Порядок проведения периодических проверок состояния организации обработки и обеспечения безопасности ПДн

12.1 Организация проведения проверок

12.1.1 Периодические проверки состояния организации обработки и обеспечения безопасности ПДн осуществляются в целях внутреннего контроля соответствия обработки ПДн установленным требованиям законодательства РФ о ПДн и локальным актам.

12.2 Внутренние проверки проводятся:

(1) лицом, ответственным за организацию обработки ПДн;

(2) лицом, ответственным за обеспечение безопасности ПДн в ИСПДн;

(3) комиссией по проведению внутреннего контроля соответствия организации обработки и обеспечения безопасности ПДн, формируемой руководителем.

12.2.1 Содержание проверок, их периодичность и ответственные исполнители определены в плане внутренних проверок состояния организации обработки и обеспечения безопасности ПДн.

12.2.2 Результаты проверки оформляются в виде акта, который содержит:

(1) указание на период проведения проверки;

(2) описание нарушений и недостатков, выявленных в процессе проверки;

(3) предложения и рекомендации по снижению рисков, устранению недостатков и повышению эффективности внутреннего контроля.

12.2.3 По результатам проведения проверок, при необходимости, формируется и утверждается план устранения недостатков, выявленных в ходе проверок, содержащий следующие сведения:

(1) выявленные недостатки;

(2) наименование мероприятий по устранению недостатков;

(3) срок проведения мероприятий;

(4) наименование ответственных лиц;

(5) перечень ожидаемых результатов устранения недостатков.

12.2.4 Контроль за устранением выявленных недостатков осуществляется лицом, ответственным за организацию обработки ПДн, посредством запроса информации у лиц, ответственных за реализацию мероприятий по устранению недостатков и иными способами, предусмотренными локальными актами.

13 Порядок проведения оценки вреда субъектам, ПДн которых обрабатываются

13.1 Методика проведения оценки вреда, который может быть причинен субъектам ПДн

13.1.1 Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ, осуществляется лицом, ответственным за организацию обработки ПДн, в соответствии с методикой, описанной в данном разделе Положения.

13.1.2 Согласно ч.2 ст.17 152-ФЗ вред субъекту ПДн может быть причинен в следующих формах:

(1) убытки[2] – расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода);

(2) моральный вред[3] – физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

13.1.3 Оценка вреда, который может быть причинен субъектам ПДн, проводится на основании следующей шкалы:

(1) низкий уровень вреда – нарушение прав субъектов ПДн может привести к незначительным негативным последствиям для субъектов ПДн (далее – «**Н**»);

(2) средний уровень вреда – нарушение прав субъектов ПДн может привести к негативным последствиям для субъектов ПДн (далее – «**С**»);

(3) высокий уровень вреда – нарушение прав субъектов ПДн может привести к значительным негативным последствиям для субъектов ПДн (далее – «**В**»).

13.1.4 Оценка возможного вреда субъектам ПДн определяется на основании экспертных значений, с использованием информации о категории, объёме и принадлежности ПДн, обрабатываемых Компанией.

13.2 Правила соотнесения возможного вреда субъектам ПДн и реализуемых мер

13.2.1 Соотнесение лицом, ответственным за организацию обработки ПДн, возможного вреда субъектам ПДн и реализуемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ.

13.2.2 Состав реализуемых правовых, организационных и технических мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ, определяется лицом, ответственным за организацию обработки ПДн, исходя из правомерности и разумной достаточности указанных мер.

14 Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

[2] См. ч.2 ст.15 ГК РФ.
[3] См. ст.151 ГК РФ.

14.1 Случаи привлечения к ответственности

14.1.1 Сотрудники, виновные в нарушении норм, регулирующих обработку ПДн, несут административную ответственность согласно ст.ст.13.11, 13.14 КоАП РФ.

14.1.2 Предоставление ПДн посторонним лицам, в том числе, сотрудникам, не имеющим права их обрабатывать, распространение ПДн, утрата материальных носителей информации, содержащих ПДн субъекта, а также иные нарушения обязанностей по обработке ПДн, установленных Положением, локальными актами, влечет наложение на сотрудника, имеющего доступ к ПДн, дисциплинарного взыскания: замечания, выговора или увольнения.

14.1.3 Сотрудник, имеющий доступ к ПДн субъектов и совершивший вышеуказанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба (п.7 ст.243 ТК РФ).

14.1.4 Сотрудники, имеющие доступ к ПДн субъектов, виновные в незаконном сборе или передаче ПДн, а также осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со ст.ст.137, 272 УК РФ.