УТВЕРЖДАЮ

Директор
ОБУК «Госдирекция»

_____А.А. Найденов

«_а_» _____ 20_21_ г.

МП

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных и технология обработки персональных данных

Липецк 2021

Оглавление

1. Термины, определения и сокращения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Автоматизированная система (АС) – Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

2. Общие положения

2.1. Настоящая инструкция разработана на основании следующих нормативных документов:

2.1.1. Федеральный закон от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2.1.2. Федеральный закон от 27 июня 2006 № 152 «О персональных данных»;

2.1.3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

2.1.4. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.1.5. Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

2.1.6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

2.1.7. Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.

2.1.8. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 30 июля 2012 г. N 240/24/3095 «Об утверждении требований к средствам антивирусной защиты»;

2.1.9. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 20 ноября 2012 г. N 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных»;

2.1.10. Информационное сообщение Федеральной службы по техническому и экспортному контролю от 15 июля 2013 г. N 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"».

2.2. Настоящая инструкция определяет основные задачи, функции, обязанности, права и ответственность пользователей информационных систем (далее – ИС) ОБУК «Госдирекция» (далее – Организация).

2.3. Средства вычислительной техники (далее – СВТ) разрешается использовать для обработки информации, содержащей персональные данные (далее – ПДн), при соблюдении следующих условий:

2.3.1. Вспомогательные технические средства и системы (далее – ВТСС), провода и кабели располагать от основных технических средств и систем (далее – ОТСС) в соответствии с Предписаниями на эксплуатацию.

2.3.2. Подключение ОТСС осуществлять с использованием штатных кабелей.

2.3.3. Право работы на персональной электронно-вычислительной машине (далее – ПЭВМ) предоставляется Администратору безопасности ИС и пользователям в соответствии с «Матрицей доступа пользователей к персональным данным».

2.3.4. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению (далее – ПО) и данным ПЭВМ, несет персональную ответственность за свои действия.

3. Обязанности пользователя ИСПДн

3.1. Выполнять на ПЭВМ только те процедуры, которые определены для него в системе доступа к информационным (программным) ресурсам объекта информатизации.

3.2. Знать и соблюдать установленные требования по режиму обработки ПДн, их учету и хранению.

3.3. Знать и соблюдать требования законодательства Российской Федерации в области защиты ПДн.

3.4. Пользователи перед началом обработки на ПЭВМ файлов, хранящихся на съемных носителях информации (далее – НИ), должны осуществить проверку файлов на наличие компьютерных вирусов.

3.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.6. Соблюдать установленный режим разграничения доступа к информационным ресурсам.

3.7. Получать у Администратора безопасности идентификатор, надежно его хранить в сейфе.

3.8. Получать у Администратора безопасности пароль, надежно его хранить в тайне.

3.9. Немедленно докладывать Администратору безопасности обо всех фактах и попытках НСД к обрабатываемой на ПЭВМ информации или об ее исчезновении (искажении).

3.10. Пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Del и кнопки «Блокировать» в появившемся меню, или выключить ПЭВМ.

3.11. Обеспечивать сохранность материалов с ПДн. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с ПДн в закрываемые на замок сейфы, шкафы, столы, и т.п.

3.12. При работе с документами, содержащими ПДн, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними.

3.13. Немедленно сообщать ответственному за организацию обработки ПДн о недостаче, утрате, утечке или искажении ПДн, об обнаружении неучтенных материалов с указанной информацией.

3.14. Предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации и нормативными актами, по их требованию все числящиеся и имеющиеся в наличии документы по защите ПДн.

3.15. Пользователям ИСПДн запрещается:

3.15.1. записывать и хранить информацию на неучтенных НИ;

3.15.2. оставлять во время работы НИ (или ПЭВМ с НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;

3.15.3. хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

3.15.4. хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;

3.15.5. самостоятельно отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на данной ПЭВМ;

3.15.6. обрабатывать информацию с выключенным или нефункционирующими устройствами защиты информации;

3.15.7. вносить изменения в настройку средств защиты информации ИСПДн.

3.15.8. производить какие-либо изменения в электрических схемах, монтаже и размещении ОТСС и ВТСС;

3.15.9. самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования ОТСС и ВТСС;

3.15.10. обрабатывать на ПЭВМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;

3.15.11. оставлять включенными ПЭВМ с предоставленными правами доступа к ИСПДн, после окончания работы (в перерывах);

3.15.12. сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ПЭВМ;

3.15.13. записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

3.15.14. работать на ПЭВМ при обнаружении каких-либо неисправностей;

3.15.15. вводить ПДн под диктовку или с микрофона;

3.15.16. осуществлять электропитание и заземление ОТСС от нештатных сетей электропитания и заземления;

3.15.17. привлекать посторонних лиц для осуществления ремонта ОТСС без согласования с ответственным за организацию обработки ПДн;

3.15.18. сообщать информацию о ПДн лицам, не имеющим права доступа к ней;

3.15.19. выносить документы и иные материалы с ПДн, а также их копии из служебных помещений, предназначенных для работы с ними.

4. Технология обработки персональных данных

4.1. При первичном допуске к работе на ПЭВМ пользователи знакомятся с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки ПДн.

4.2. Пользователь включает ПЭВМ, визуально убеждается в целостности наклеек, исправности и нормальном функционировании ПЭВМ.

4.3. В процессе работы пользователи создают файлы и массивы информации на ПЭВМ.

4.4. При необходимости вывод персональных данных из ПЭВМ осуществляется следующим образом:

- копированием на учтенные носители;
- на печатающее устройство.

5. Порядок учета, хранения и выдачи носителей ПДн

5.1. **Хранение носителей**

5.1.1. ПДн Субъекта, хранимые на машинных носителях, находятся в ведении подразделений Организации, осуществляющих эксплуатацию данных автоматизированных рабочих мест или машинных носителей, используемых в информационной системе для хранения и обработки информации. Допуск к ПДн имеют работники Организации, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей.

5.1.2. В целях недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5.1.3. Материальные носители ПДн, представленных в бумажном виде, должны храниться в сейфе, в запираемом металлическом шкафу или другим способом, исключающим несанкционированный доступ. Организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5.2. **Учет носителей**

5.2.1. При учете носителей реализуются следующие требования обеспечения защиты персональных данных:

– формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;

– предупреждение возможности нецелевого использования носителя или его неправильного хранения;

– формирование грифа конфиденциальности будущего документа;

– предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, частей фото-, видео- или магнитной пленки), для чего

фиксируются технические характеристики носителя (количество листов, длина ленты, наличие склеек и др.);

– включение носителя в сферу регулярного контроля сохранности и местонахождения;

– предотвращение выдачи носителя лицу, исключенному из состава лиц, допускаемых к данному носителю (составляемому документу);

– выявление факта утраты носителя или его частей, организация поиска носителя и проведения служебного расследования;

– предотвращение нарушения принципа персональной ответственности за сохранность носителя и фиксируемых в нем персональных данных;

– обнаружение факта подмены носителя другим, фальсификации части носителя;

– обнаружение фактов случайной или умышленной порчи носителя, изменения формата, нумерации листов, вырывания листов, их загрязнения, склеивания и т.п.;

– предотвращение несанкционированной и неоправданной деловой необходимостью передачи носителя между руководителями и исполнителями;

– предотвращение несанкционированного ознакомления посторонних лиц с содержанием информации, зафиксированной на носителе, в процессе его выдачи исполнителю и прием от исполнителя.

5.2.2. Машинные носители подлежат учету. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

5.2.3. Учет съемных машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства) информации ведется в журналах учета машинных носителей информации. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш- накопители, съемные жесткие диски).

5.2.4. Учет встроенных в портативные или стационарные технические средства машинных носителей информации (накопители на жестких дисках) может вестись в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

5.2.5. Регистрационные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или пользователей, которым разрешен доступ к машинным носителям информации для выполнения своих должностных обязанностей (функций). При необходимости учетные данные переносятся на носитель и его составные части для их идентификации (на CD-R, CD-RW диски).

5.2.6. Материальные носители ПДн, представленные в бумажном виде, регистрируются в журналах материально-технического учета. Регистрационные данные переносятся на носитель и его составные части для их идентификации.

5.2.7. Правильность учета носителей и их наличие проверяется ежедневно.

5.3. **Выдача носителей**

5.3.1. Выдача учтенного, укомплектованного носителя информации сотруднику включает закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование.

5.3.2. Прием от исполнителя носителя информации включает проверку комплектности носителя, наличия оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя.

6. Идентификация и аутентификация пользователей информационных систем

6.1. Настройки средств защиты от несанкционированного доступа должны осуществлять идентификацию и аутентификацию при доступе в ИС пользователей, являющихся работниками в Организации (внутренних пользователей), пользователей, не являющихся работниками оператора (внешних пользователей),и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

6.2. В качестве внутренних пользователей рассматриваются должностные лица (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС в соответствии с должностными регламентами (инструкциями) утвержденными Руководителем Организации и которым в ИС присвоены учетные записи, и, дополнительно, должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной ИС, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) и которым в ИС также присвоены учетные записи.

6.3. К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все остальные пользователи ИС, не указанные в качестве внутренних пользователей.

6.4. Пользователи ИС должны однозначно идентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до прохождения ими процедур идентификации и аутентификации.

6.5. Ответственность за создание, присвоение и уничтожение идентификаторов и средств аутентификации пользователей и устройств несет Администратор безопасности. Администратор безопасности проверяет на СВТ пользователя заданные возможности доступа и выдает пользователю под расписку в соответствующем журнале учета его персональный идентификатор.

6.6. Функционал, доступный до прохождения процедур идентификации и аутентификации

6.6.1. При предоставлении доступа к персональным данным и любой иной конфиденциальной информации пользователям запрещены любые действия до прохождения ими процедур идентификации и аутентификации.

6.6.2. При предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам) до прохождения процедур идентификации и аутентификации доступны функции чтения и копирования.

6.7. Пользователи ИС должны однозначно аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до прохождения ими процедур идентификации и аутентификации.

6.8. Аутентификация пользователей осуществляется с использованием паролей, аппаратных средств, или - определенной комбинации указанных средств.

6.9. Администратор устанавливает и реализует следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе.

6.10. Владельцы паролей должны быть ознакомлены под роспись с требованиями к организации парольной защиты и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации (личный пароль пользователь не имеет права сообщать никому).

6.11. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы персональных данных в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

6.12. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6.10. или п.6.11. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

6.13. Хранение пользователем значений своих паролей на бумажном носителе допускается только в личном опечатанном сейфе, либо в сейфе у ответственного за организацию обработки персональных данных.

7. Порядок подключения рабочих станций к сети общего пользования

7.1. Информационно-вычислительная сеть общего пользования является открытой системой передачи данных, при работе в которой могут возникнуть следующие основные угрозы:

- заражение СВТ программными вирусами;
- несанкционированный доступ внешних пользователей к ПДн;
- внедрение программных закладок;
- загрузка трафика нежелательной корреспонденцией (спамом);
- несанкционированная передача ПДн пользователями ИСПДн в сети общего пользования.

7.2. Для предотвращения указанных угроз реализуется:

- разграничение доступа пользователей к ресурсам информационно-вычислительных сетей путём использования средств межсетевого экранирования защищённого сегмента локальной вычислительной сети, в котором происходит обработка ПДн;
- осуществление контроля за персональными данными, выходящими из информационных систем Организации в сети общего пользования;
- применение средств криптографии при использовании сетей связи общего пользования для передачи информации, содержащей персональные данные.

7.3. Пользователям, рабочие станции которых подключены к сети общего пользования для доступа к ресурсам Интернет и электронной почты, разрешается использовать лишь те ресурсы, которые необходимы для выполнения их функциональных обязанностей.

7.4. Подключение рабочих станций пользователей Организации к сети общего пользования для доступа к ресурсам Интернет и электронной почты, осуществляется по решению директора Организации.

7.5. После получения разрешения производится:

— установка и настройка необходимого программного обеспечения для доступа к ресурсам сетей общего пользования;

— конфигурирование системы контроля доступа в соответствии с политикой безопасности;

— присвоение пользователям персональных идентификаторов;

— выработка каждому пользователю пароля, при этом пароль должен быть индивидуален для каждого пользователя, быть трудно подбираемым и не сочетаться с именем пользователя.

8. Передача персональных данных

8.1. При передаче персональных данных необходимо соблюдать следующие требования:

8.1.1. не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

8.1.2. не сообщать ПДн в коммерческих целях без его письменного согласия;

8.1.3. предоставлять доступ к ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн, которые необходимы для выполнения их функциональных обязанностей;

8.1.4. в случае, если Организация на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности ПДн и безопасности ПДн при их обработке.

8.2. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, не осуществляется.

9. Прием персональных данных

9.1. Получение Организацией ПДн Субъекта производится одним из ниже перечисленных способов:

9.1.1. Субъект ПДн непосредственно принимает решение о предоставлении ПДн и дает письменное согласие на их обработку Организацией. Форма заявления-согласия субъекта на обработку ПДн представлена в Приложении №1 к Правилам обработки персональных данных (на примере согласия работника на обработку ПДн).

9.1.2. В случае недееспособности Субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн. В случае получения согласия на обработку ПДн от представителя Субъекта ПДн, полномочия данного представителя на дачу согласия от имени Субъекта ПДн должны проверяться Организацией.

9.1.3. В случае смерти Субъекта ПДн согласие на обработку его ПДн дают наследники Субъекта ПДн, если такое согласие не было дано Субъектом ПДн при его жизни.

9.1.4. ПДн так же могут быть получены от лица, не являющегося Субъектом ПДн, при условии наличия оснований для обработки ПДн из указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27 июля 2006 г. «О персональных данных». Например, письменное согласие Субъекта ПДн не требуется, если обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является Субъект ПДн.

9.2. Согласие на обработку ПДн может быть отозвано Субъектом ПДн или, в случае недееспособности Субъекта ПДн, законным представителем Субъекта ПДн. Форма отзыва согласия на обработку ПДн представлена в Приложении № 2 к настоящим Правилам. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27 июля 2006 г. «О персональных данных».

9.3. При приеме персональных данных должно соблюдаться следующее требование: если ПДн были получены не от субъекта ПДн, за исключением случаев, если ПДн были предоставлены Организации на основании федерального закона или если ПДн являются общедоступными, необходимо до начала обработки таких ПДн убедиться в том, что передающая сторона письменно уведомила субъект ПДн о факте передачи его ПДн в адрес Организации. Если уведомление отсутствует, или факт его наличия установить не представляется возможным необходимо предоставить субъекту ПДн следующую информацию:

9.3.1. наименование либо фамилия, имя, отчество и адрес Организации или её представителя;

9.3.2. цель обработки ПДн и ее правовое основание;

9.3.3. предполагаемые пользователи ПДн;

9.3.4. установленные Федеральным законодательством Российской Федерации права субъекта ПДн;

9.3.5. источник получения ПДн.

9.4. Организация освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные п.9.1., в случаях, если:

9.4.1. субъект ПДн уведомлен об осуществлении обработки его ПДн Организацией;

9.4.2. ПДн получены Организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

9.4.3. ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

9.4.4. Организация осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

9.4.5. предоставление субъекту ПДн сведений, предусмотренных п.9.1., нарушает права и законные интересы третьих лиц.

9.5. Порядок учета, обработки и передачи принятых ПДн осуществляется в соответствии с нормами, установленными для ПДн, находящихся в Организации на постоянной основе.

10. Приостановление обработки и уничтожение персональных данных

10.1. В случае выявления факта неправомерной обработки ПДн при обращении или по запросу Субъекта ПДн (его представителя или уполномоченного органа по защите прав субъектов персональных данных) Организация обязана осуществить блокирование неправомерно обрабатываемых ПДн с момента такого обращения или получения указанного запроса на период проверки.

10.2. В случае выявления неправомерной обработки ПДн, осуществляемой Организацией или лицом, действующим по поручению Организации, Организация в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн. В случае, если обеспечить правомерность обработки ПДн невозможно, Организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязана обеспечить уничтожение таких ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Организация уведомляет Субъект ПДн или его представителя, а в случае, если обращение Субъекта ПДн или его представителя было направлено уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

10.3. В случае достижения цели обработки ПДн Организация обеспечивает прекращение обработки ПДн и их уничтожение в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Организацией и Субъектом ПДн либо если Организация не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных федеральным законодательством. Форма Акта об уничтожении персональных данных субъекта персональных данных (в случае достижения целей обработки) представлена в Приложении № 6 к Правилам обработки персональных данных.

10.4. В случае отзыва Субъектом ПДн согласия на обработку его ПДн Организация обеспечивает прекращение их обработки и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, обеспечивает уничтожение ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором или иным соглашением между Организацией и Субъектом ПДн либо если Организация не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных федеральным законодательством. Форма заявления Субъекта ПДн о прекращении обработки и уничтожении персональных данных представлена в Приложении № 2 к Правилам обработки персональных данных.

10.5. В случае отсутствия возможности уничтожения ПДн, оператор первоначально обеспечивает блокирование таких ПДн, а в дальнейшем – уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

10.6. 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).

10.7. Специализированными средствами или методами гарантированного уничтожения информации сотрудниками Организации обеспечивается уничтожение (стирание) информации на цифровых и нецифровых, съемных и несъемных машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также производится контроль уничтожения (стирания) информации для исключения возможности восстановления защищаемой информации при передаче носителей.

10.8. В случае прекращения полномочий работника Администратором безопасности ИСПДн приостанавливается предоставление ему персональных данных, а также немедленно производиться смена пароля после окончания последнего сеанса работы данного пользователя с системой.

11. Порядок проведения внутреннего расследования по фактам разглашения персональных данных

11.1. В случае утраты ПДн работником, либо возникновения утечки ПДн по иным причинам, в Организации проводится внутреннее расследование.

11.2. Работник, по вине которого произошло нарушение, обязан по требованию Ответственного за организацию обработки персональных данных представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный за организацию обработки персональных данных вправе увеличить указанный срок, а также поставить перед работником перечень вопросов, на которые работник обязан ответить.

11.3. В целях внутреннего расследования все работники обязаны по первому требованию Ответственного за организацию обработки персональных данных предъявить для проверки все числящиеся за ними материалы, содержащие ПДн, представить устные или письменные объяснения, в том числе об известных им фактах разглашения ПДн, утраты документов и изделий, содержащих ПДн.

11.4. В случае давления на работника со стороны других работников или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом ответственному за организацию обработки персональных данных.

11.5. Для проведения внутреннего расследования Руководитель вправе создать комиссию из опытных и квалифицированных работников в составе не менее трех человек.

11.6. В процессе проведения внутреннего расследования выясняются:

11.6.1. перечень разглашенных сведений, составляющих персональные данные;

11.6.2. причины разглашения персональных данных;

11.6.3. круг лиц, виновных в разглашении персональных данных;

11.6.4. размер причиненного ущерба;

11.6.5. недостатки и нарушения, допущенные работниками при работе с персональными данными;

11.6.6. иные обстоятельства.

11.7. По результатам расследования, комиссией составляется акт, с отражением в нем лиц, виновных в разглашении персональных данных, размера причиненного ущерба Организации, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

11.8. На основании акта выносится решение о:

11.8.1. применении мер дисциплинарного воздействия к работнику;

11.8.2. информировании регулятора о факте нарушения;

11.8.3. информировании правоохранительных органов;

11.8.4. информировании субъектов персональных данных.

11.9. После вынесения решения работник имеет право знакомиться с актом внутреннего расследования и иными материалами.

10. Порядок применения средств антивирусной защиты информации

10.1. В организации обеспечивается антивирусная защита информационных систем, включающая обнаружение компьютерных программ либо иной компьютерной информации,

предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

10.2. Средства антивирусной защиты информации должны устанавливаться на всех автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).

10.3. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

10.4. В информационной системе прав по управлению (администрированию) средствами антивирусной защиты предоставляются только администратору безопасности.

10.5. Реализация антивирусной защиты должна предусматривать:

10.5.1. установку, конфигурирование и управление средствами антивирусной защиты, исполняемая Администратором безопасности.

10.5.2. предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

10.5.3. проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов) по предварительному согласованию с Администратором безопасности;

10.5.4. проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

10.5.5. проведение внеплановых проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) в случае подозрения на наличие программных вирусов;

10.5.6. оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

10.5.7. выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами);

10.5.8. обновление базы данных признаков вредоносных компьютерных программ (вирусов) по предварительному согласованию с Администратором безопасности или в автоматическом режиме.

10.6. Пользователям запрещается:

10.6.1. отключать средства антивирусной защиты информации во время работы;

10.6.2. без разрешения Администратора безопасности копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

10.7. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом Администратора безопасности. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом администратору безопасности

10.8. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений пользователь должен:

10.8.1. приостановить процесс приема-передачи информации;

10.8.2. сообщить Администратору безопасности о факте обнаружения программного вируса;

10.8.3. принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

10.9. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

10.9.1. немедленно приостановить все работы;

10.9.2. сообщить Администратору безопасности о факте обнаружения программных вирусов;

10.9.3. принять по согласованию с Администратором безопасности меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

10.10. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования.

11. Порядок реагирования на инцидент

11.1. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

11.1.1. **Уровень 1 – Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

11.1.2. **Уровень 2 – Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

11.1.3. **Уровень 3 – Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИСПДн и средств защиты на сутки и более.

11.2. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

11.2.1. системы жизнеобеспечения;

11.2.2. системы обеспечения отказоустойчивости;

11.2.3. системы резервного копирования и хранения данных;

11.2.4. системы контроля физического доступа.

11.3. Системы жизнеобеспечения ИСПДн включают:

11.3.1. пожарные сигнализации и системы пожаротушения;

11.3.2. системы вентиляции и кондиционирования;

11.3.3. системы резервного питания.

11.4. Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

11.5. Для обеспечения возможности восстановления программного обеспечения в информационной системе приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций (Инструкция по действиям персонала в нештатных ситуациях).

Председатель ПДК А.А. Найденов

«01» августа 2021 г.

Приложение 1

Лист ознакомления

№ п/п	Ф.И.О.	Роспись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		