**УТВЕРЖДАЮ**

**Директор**
**ОБУК «Госдирекция»**

**_____А.А. Найденов**

**«01» октября 2021 г.**

МП

# ИНСТРУКЦИЯ

**ответственного за организацию 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:

- Федеральный закон от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июня 2006 № 152 «О персональных данных»;
- 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»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 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»;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.
- 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»;
- 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»;
- 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. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за организацию обработку персональных данных в информационных системах (далее – Ответственного) ОБУК «Госдирекция» (далее – Организация).

2.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных в информационных системах (далее – ИС) (указанных в п. 2.1.) и обеспечивает их выполнение.

2.4. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации.

## 3. Задачи и функции Ответственного

3.1. Основными задачами Ответственного являются:

- разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн;
- доведение до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление внутреннего контроля за соблюдением требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- контроль эффективности защиты информации.

3.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

3.2.1. Организация допуска пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИС в соответствии с «Матрицей доступа пользователей к защищаемым персональным данным ИС» на всех стадиях жизненного цикла ИС.

3.2.2. Участие на стадии проектирования (внедрения) ИС, в разработке технологии обработки персональных данных по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;
- подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ИС по вопросам защиты персональных данных, а также ответственных по защите персональных данных в процессе их автоматизированной обработки.

3.2.3. Контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке персональных данных в ИС.

3.2.4. Оперативный контроль за ходом технологического процесса обработки персональных данных.

3.2.5. Методическое руководство работой пользователей ИС в вопросах обеспечения информационной безопасности.

## 4. Обязанности Ответственного

4.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

4.1.1. Разработать и вести:

— Журнал по учету мероприятий по контролю обеспечения защиты персональных данных в ИС;

— Журнал учета носителей персональных данных;

— Журнал учета передачи персональных данных;

— Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации;

— Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

4.1.2. Разработать перечень ПДн.

4.1.3. Разрабатывать решения по:

— составу рабочей группы в защищаемом сегменте сети, системы доверительных отношений между членами группы;

— определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

— определению списка устройств, логических дисков, каталогов общего пользования на серверах с указанием состава допущенных к ним пользователей и режимом допуска;

— разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, использованию СЗИ при передаче конфиденциальных документов).

4.1.4. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ПЭВМ, на которых ведется обработка ПДн.

4.1.5. Своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ.

4.1.6. Контролировать обеспечение защиты персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

4.1.7. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

4.1.8. Контролировать эффективность защиты персональных данных:

- Проводить работу по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ.
- Проводить занятия с администраторами и пользователями ИС по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по

вопросам обеспечения безопасности информации с разбором недостатков выявленных при контроле эффективности защиты информации.

4.1.9. Организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования.

4.1.10. Осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

4.1.11. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

4.2. Ответственному запрещается:

4.2.1. Использовать в своих и в чьих-либо личных интересах ресурсы ИС, предоставлять такую возможность другим.

4.2.2. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИС, блокировке, потери информации и предупреждения пользователей.

4.2.3. Допускать к работе на ПЭВМ и серверах посторонних лиц.

## 5. Права Ответственного

5.1. Ответственный имеет право:

- Получать доступ к программным и аппаратным средствам ИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИС и ПЭВМ пользователей.
- Требовать от пользователей ИС выполнения инструкций по обеспечению безопасности персональных данных в ИС.
- Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС.
- Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом Руководителю.

5.2. Лицо, ответственное за организацию обработки ПДн, несет ответственность за:

- Реализацию утвержденных в Организации документов, регламентирующих порядок обеспечения безопасности персональных данных.
- Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним Руководителем и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.
- Разглашение персональных данных и сведений ограниченного распространения, ставших известными ему по роду работы.
- Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИС.

## 6. Порядок учета, хранения и выдачи носителей персональных данныхн

6.1. Ответственный организует учет, хранение и выдачу носителей ПДн.

6.2. Хранение носителей

6.2.1. 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.

6.2.2. 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.

6.2.3. 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.

6.3. Учет носителей

6.3.1. 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.

6.3.2. 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.

6.3.3. 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).

6.3.4. 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.

6.3.5. 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).

6.3.6. 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.

6.3.7. Правильность учета носителей и их наличие проверяется ежедневно.

6.4. Выдача носителей

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

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

## 7. Порядок применения средств организации архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных

7.1. Ответственный осуществляет контроль за процессом архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных.

7.2. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в Организации.

7.3. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения устанавливается с учетом соблюдения следующих требований:

- обязательное хранение всех архивов в защищенном месте;
- частота архивации данных зависит от их важности и частоты их изменения;
- системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;
- данные, которые изменяются очень редко, не имеет смысла архивировать.
- восстановление работоспособности программных средств и информационных массивов, в случае утери и повреждения.

7.4. Организации архивирования и восстановления прикладного программного обеспечения подлежат следующие файлы и документы:

- все файлы операционной системы и установленных приложений. Архивирование системных файлов должно производиться только после установки новых приложений или обновления самой операционной системы;
- личные профили пользователей;
- папки, содержащие важные документы;
- базы данных;
- другие файлы и папки, представляющие ценность.

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

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

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

7.7. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

7.8. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы;
- системы обеспечения отказоустойчивости (кластеризация; технология RAID).

7.9. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

7.10. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

7.11. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

7.12. Носители должны храниться не менее года, для возможности восстановления данных.

## 8. Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных.

8.1. Основными целями проведения внутреннего расследования являются:

- выявление предпосылок утраты персональных данных в результате нарушения порядка их обработки;
- выявления лиц из числа сотрудников Организации виновных в утрате персональных данных;
- определение ущерба в результате утраты персональных данных;

- проверка полноты и качества исполнения нормативных документов по работе со средствами защиты персональных данных;
- документальное подтверждение соответствия обработки, хранения и передачи персональных данных нормам и правилам, установленным федеральными правовыми и нормативными актами;
- определение фактического состояния системы защиты персональных данных.

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

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

8.4. 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.

8.5. Для проведения внутреннего расследования Руководитель формирует комиссию из опытных и квалифицированных работников в составе не менее трех человек.

8.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным работникам Организации о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

8.7. В процессе проведения внутреннего расследования выясняются:
- перечень разглашенных сведений, составляющих персональные данные;
- причины разглашения персональных данных;
- круг лиц, виновных в разглашении персональных данных;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с персональными данными;
- иные обстоятельства.

8.8. 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.

8.9. На основании акта комиссия выносит решение о:
- применении мер дисциплинарного воздействия к работнику;

- информировании регулятора о факте нарушения;
- информировании правоохранительных органов;
- информировании субъектов персональных данных.

## 9. Порядок реагирования на аварийную ситуацию

9.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС.

9.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться Ответственным в «Журнале по учету мероприятий по контролю».

9.3. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный за реагирование предпринимает меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

9.4. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИС и средств защиты.
- Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС и средств защиты.
- Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС и средств защиты, а также к угрозе жизни пользователей ИС, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИС и средств защиты на сутки и более.

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

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

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

9.7. Ответственным должно быть проведено обучение должностных лиц, имеющих доступ к ресурсам ИС, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

9.8. Администратор безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИС.

9.9. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

## 10. Организация режима безопасности помещений, где осуществляется работа с персональными данными

10.1. Первичный (основной) метод – система контроля и управления доступом в здание организации, включает в себя:

- наличие при входе в здание пункта контрольного пропуска;
- наличие ведомственной службы охраны;
- определение внешнего контролируемого периметра.

10.2. Вторичный (дополнительный) метод – система контроля перемещения лиц в здании и управления доступом в помещения, включает в себя:

- наличие помещений с активным сетевым оборудованием с определенными правами доступа;
- наличие охранной и пожарной сигнализаций в помещениях Организации;
- использование кодовых замков и иных технических средств ограничения доступа в помещения;
- использование сейфов, шкафов, а также хранение информации с ПДн на внутренних и внешних носителях.

10.3. Ограничение доступа посторонних лиц в помещения, предназначенные для осуществления профессиональной деятельности, связанной с эксплуатацией ИС, предусматривает следующие:

- Исключение возможности бесконтрольного проникновения в эти помещения посторонних лиц, включая работников других структурных подразделений.
- После окончания рабочего дня двери помещений, в которых эксплуатируется ИС, закрываются на ключ и опечатывается персональным пломбиром. Все помещения имеют разные замки. Дубликаты ключей хранятся в запираемом шкафу у Ответственного. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.
- Уборка помещения производится в присутствии одного из сотрудников, работающего в этом помещении.
- Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.
- Строгое ограничение доступа посторонних лиц к серверам, а также сетевому оборудованию.
- Защита мест хранения носителей (USB flash-накопитель, CD, НЖМД) от беспрепятственного доступа посторонних лиц.

## 11. Приостановление обработки персональных данных

11.1. При выявлении недостоверных персональных данных или неправомерных действий с ними при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных (приостановки предоставления персональных данных пользователям ИС), с момента такого обращения или получения такого запроса на период проверки.

11.2. В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов требуется уточнить персональные данные и снять их блокирование.

11.3. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

11.4. В случае достижения цели обработки персональных данных необходимо незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъект персональных данных или его законного представителя, а в случае,

если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

11.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных требуется прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Организацией и субъектом персональных данных. Об уничтожении персональных данных необходимо уведомить субъект персональных данных.

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

Директор ОБУК «Госдирекция» _____ А.А. Найденов
(должность) (подпись) (ФИО)

«01» октября 2021 г.

С инструкцией ознакомлен:

И. о. чена _____ _____ А. С. Пикабы
_____
(должность) (подпись)
(ФИО)

«01» октября 2021 г.