УТВЕРЖДАЮ

Директор
ОБУК «Госдирекция»

_____А.А. Найденов

«01» 09 2021 г.

МП

ИНСТРУКЦИЯ

администратора безопасности информационных систем

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 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

2.1.3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 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. № 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. № 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. № 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. № 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. № 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, права и ответственность Администратора безопасности информационных систем (далее – ИС) ОБУК «Госдирекция» (далее – Организация).

2.3. Администратор безопасности выполняет функции по обеспечению бесперебойного функционирования систем защиты ИС.

2.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом директора организации.

2.5. В своей деятельности Администратор безопасности руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных (указанных в п. 2.1.) и обеспечивает их выполнение.

2.6. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации и не исключает обязательного выполнения их требований.

3. Задачи и функции Администратора безопасности

3.1. Основными задачами Администратора безопасности являются:

3.1.1. сопровождение средств защиты информации, основных технических средств и систем (далее - ОТСС), носителей ПДн в соответствии с эксплуатационной документацией;

3.1.2. обеспечение работоспособности элементов ИС и локальной вычислительной сети;

3.1.3. организация разграничения доступа пользователей к информационным ресурсам.

3.2. Для выполнения поставленных задач на Администратора безопасности возлагаются следующие функции:

3.2.1. Настройка и сопровождение средств защиты от несанкционированного доступа (далее НСД), в том числе средств криптографической защиты информации в ИС.

3.2.2. Учет лиц, допущенных к работе с персональными данными, идентификация и аутентификация пользователей информационных систем. Ведение списка пользователей ИС в информационной базе системы защиты от НСД, их полномочий доступа (чтение, запись) к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИС. Назначение и смена паролей к информационным ресурсам ИС.

3.2.3. Настройка и сопровождение подсистемы регистрации и учета:

- ввод в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
- проведение регулярного анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременное информирование руководства о несанкционированных действиях персонала и организация расследования попыток НСД.

3.2.4. Сопровождение подсистемы обеспечения целостности рабочего программного обеспечения (далее - ПО):

- регистрация и реагирование на события безопасности;
- применение средств архивирования и восстановления прикладного программного обеспечения и персональных данных;
- контроль (анализ) защищенности персональных данных;

- проведение периодического тестирования функций системы защиты от НСД, в том числе при изменении программной среды и полномочий пользователей ИС;
- восстановление системы защиты при сбоях;
- контроль соответствия общесистемной программной среды эталону.

3.2.5. Поддержание установленного порядка и соблюдение требований антивирусной защиты.

3.2.6. Организация обучения пользователей.

3.2.7. Организация учета, хранения и выдачи носителей ПДн.

3.2.8. Организация учета средств защиты информации, средств криптографической защиты информации, эксплуатационной и технической документации к ним.

3.2.9. Организация установки и обновления программного обеспечения.

3.2.10. Организация обмена персональными данными со сторонними организациями.

3.2.11. Организация подключения рабочих станций к сетям общего пользования.

4. Права и ответственность Администратора безопасности

4.1. Администратор безопасности имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам ИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИС и рабочих станций пользователей.

4.1.2. Требовать от пользователей ИС выполнения инструкций по обеспечению безопасности персональных данных в ИС.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС.

4.1.4. 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 докладом ответственному за организацию обработки персональных данных.

4.1.5. Производить анализ защищенности ИС и попыток взлома системы защиты ИС путем применения специальных средств.

4.1.6. Вносить свои предложения по совершенствованию мер защиты в ИС.

4.1.7. Для обеспечения незамедлительного восстановления ПДн, хранимых на машинных носителях и в ИС, в случае несанкционированной модификации или уничтожения, Администратор безопасности выполняет процедуры регулярного резервного копирования на учтенные носители, которые хранятся с исключением несанкционированного доступа к ним.

4.2. Администратор несет ответственность за:

4.2.1. Реализацию утвержденных в Организации документов, регламентирующих порядок обеспечения безопасности персональных данных.

4.2.2. Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним приказом Руководителя и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.2.3. Разглашение персональных данных и сведений ограниченного распространения, ставших известными ему при выполнении функциональных обязанностей.

4.2.4. Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИС.

4.3. Администратору безопасности запрещается:

4.3.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ее модификации, копирования, уничтожения.

4.3.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

4.3.3. Самостоятельно (без согласования с ответственным за организацию обработки персональных данных) вносить изменения в настройки серверной части ИС.

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

4.3.5. Выключать СЗИ без санкции руководства.

4.3.6. Передавать третьим лицам сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

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

4.3.8. Нарушать правила эксплуатации оборудования ИС.

4.3.9. Корректировать, удалять, подменять журналы аудита.

5. Организация учета лиц, допущенных к работе с персональными данными, идентификация пользователей информационных систем

5.1. 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.

5.2. 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.

5.3. К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все остальные пользователи ИС, не указанные в п.5.2. в качестве внутренних пользователей.

5.4. 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.

5.5. Администратор безопасности несет ответственность за создание, присвоение и уничтожение идентификаторов пользователей и устройств, выполняя следующие функции управления учетными записями:

5.5.1. определение типа учетной записи (внутреннего или внешнего пользователя; системная или приложения; гостевая (анонимная), временная и (или) иные типы записей);

5.5.2. определение используемых методов управления доступом, назначение типов доступа субъектов к объектам доступа и реализация правила разграничения доступа субъектов доступа к объектам доступа;

5.5.3. объединение учетных записей в группы (при необходимости);

5.5.4. верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

5.5.5. заведение, активация и уничтожение учетных записей пользователей, в том числе временных учетных записей и привилегированных учетных записей администраторов по Списку доступа пользователей, допущенных к работе в ИС. Список допуска пользователей ведется в специальном журнале учета (Приложение 1);

5.5.6. на основании Списка допуска Администратор безопасности разрабатывает таблицу разграничения доступа в ИС (далее - матрицу доступа): доступ к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа. Матрица доступа (Приложение 2) составляется как на электронном, так и на бумажном носителях.

5.5.7. ограничение количества неуспешных попыток доступа к информационной системе, а также обеспечено блокирование устройства и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток доступа к информационной системе;

5.5.8. обеспечение блокирования сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя. Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы) с обязательным блокированием отображения рабочего стола (использование непрозрачных хранителей экрана и т.д.). Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса;

5.5.9. выдача учетных записей пользователей, в том числе временных учетных записей и привилегированных учетных записей администраторов. Администратор безопасности проверяет на СВТ пользователя заданные возможности доступа и выдает пользователю под расписку в соответствующем журнале учета его персональный идентификатор.

5.5.10. блокирование, контроль использования, при необходимости, пересмотр и корректировка учетных записей пользователей, в том числе временных учетных записей и привилегированных учетных записей администраторов;

5.5.11. уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе. Временная учетная запись может быть заведена для пользователя на ограниченный срок для

выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе);

5.5.12. предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

5.6. Администратор безопасности назначает права и привилегии пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимые для выполнения ими своих должностных обязанностей (функций), и доступ к объектам осуществляется в соответствии с минимально необходимыми правами и привилегиями.

5.7. Функционал, доступный до прохождения процедур идентификации и аутентификации

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

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

5.7.3. Администратору разрешаются действия в обход установленных процедур идентификации и аутентификации только для восстановления функционирования информационных систем в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.8. Администратор безопасности, обеспечивающий эксплуатацию комплекса средств автоматизации, иные пользователи, допущенные к персональным данным, имеют право предоставлять такие сведения только Руководителю, а также лицам, имеющим право получать указанные сведения в соответствии с настоящей Инструкцией, соответствующими федеральными законами и другими нормативно-правовыми актами. Передавать проверяющим организациям сами персональные данные запрещается. Проверяться должны только документы, описывающие защиту.

6. Аутентификация пользователей информационных систем

6.1. 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.

6.2. Администратор несет ответственность за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

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

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

6.4.1. изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;

6.4.2. выдача средств аутентификации пользователям;

6.4.3. генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

6.4.4. установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

6.4.4.1. длина пароля не менее шести символов,

6.4.4.2. алфавит пароля не менее 60 символов,

6.4.4.3. максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток,

6.4.4.4. блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут,

6.4.4.5. смена паролей не более чем через 120 дней;

6.4.4.6. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

6.4.4.7. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

6.4.4.8. личный пароль пользователь не имеет права сообщать никому.

6.4.5. блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

6.4.6. назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

6.4.7. обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;

6.4.8. защита аутентификационной информации от неправомерного доступа к ней и модифицирования;

6.4.9. исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками"*", "• " или иными знаками.

6.5. 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.

6.6. 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.

6.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального

органа) Администратора безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИС.

6.8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 6.6. или п. 6.7. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Порядок учета средств защиты информации, средств криптографической защиты информации, эксплуатационной и технической документации к ним

7.1. Используемые средства защиты персональных данных, в т.ч. криптографические (далее – средства защиты), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету Администратором безопасности в журналах установленной формы. Средства защиты, эксплуатационная и техническая документация к ним, ключевые документы доставляются Администратором безопасности при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

7.2. Передача средств защиты, эксплуатационной и технической документации к ним между пользователями производится под расписку в соответствующем журнале.

7.3. Носители программного обеспечения, эксплуатационную и техническую документацию к ним, ключевые документы хранятся в шкафах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.4. Системные блоки рабочих станций, на которые установлены программные средства защиты, оборудуются средствами контроля за их вскрытием (опечатываются). Место опечатывания должно быть таким, чтобы его можно было визуально контролировать.

7.5. Уничтожение программных средств защиты производится Администратором безопасности по указанию органа криптографической защиты с составлением акта. Акт об уничтожении средств криптографической защиты информации (далее СКЗИ) представляется в орган криптографической защиты.

7.6. Ключевые документы уничтожаются Администратором безопасности не позднее 10 суток после вывода их из действия (окончания срока действия) с отметкой об уничтожении в соответствующем журнале.

7.7. Учет средств защиты информации производится в соответствующих журналах:

7.7.1. «Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним»;

7.7.2. «Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

8. Порядок учета, хранения и выдачи носителей ПДн

8.1. 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.

8.2. 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.

8.3. 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.

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

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

8.4.2. предупреждение возможности нецелевого использования носителя или его неправильного хранения;

8.4.3. формирование грифа конфиденциальности будущего документа;

8.4.4. 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.);

8.4.5. включение носителя в сферу регулярного контроля сохранности и местонахождения;

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

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

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

8.4.9. обнаружение факта подмены носителя другим, фальсификации части носителя;

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

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

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

8.5. 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.

8.6. 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).

8.7. 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.

8.8. 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).

8.9. 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.

8.10. Правильность учета носителей и их наличие проверяется ежедневно.

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

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

9. Порядок подключения рабочих станций к сетям общего пользования

9.1. Сеть общего пользования является открытой системой передачи данных, при работе в которой могут возникнуть следующие основные угрозы безопасности информации:

9.1.1. заражение информационно-вычислительных ресурсов программными вирусами;

9.1.2. несанкционированный доступ внешних пользователей к ресурсам информационной системы персональных данных;

9.1.3. внедрение в автоматизированные системы программных закладок;

9.1.4. загрузка трафика нежелательной корреспонденцией (спамом);

9.1.5. несанкционированная передача персональных данных пользователями ИС в сети общего пользования.

9.2. Для предотвращения указанных угроз Администратору безопасности необходимо:

9.2.1. разграничить доступ пользователей к ресурсам сетей общего пользования путём использования средств межсетевого экранирования защищённого сегмента локальной вычислительной сети, в котором происходит обработка персональных данных;

9.2.2. осуществлять контроль за персональными данными, выходящими из информационной системы Организации и загружаемых из сети общего пользования;

9.2.3. передача информации с персональными данными при использовании каналов связи сети общего пользования должна осуществляться только с применением средств криптографии.

10. Организация обмена персональными данными со сторонними организациями

10.1. При приеме и передаче персональных данных Администратор безопасности должен учитывать следующие требования:

10.1.1. коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны;

10.1.2. при конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС необходимо учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия;

10.1.3. подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием межсетевого экрана;

10.1.4. если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи.

11. Порядок применения средств антивирусной защиты информации

11.1. 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.

11.2. 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).

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

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

11.5. Реализация антивирусной защиты должна предусматривать:

11.5.1. установку, конфигурирование и управление средствами антивирусной защиты.

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

11.5.3. проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

11.5.4. 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;

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

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

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

11.5.8. обновление базы данных признаков вредоносных компьютерных программ (вирусов):

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

11.6. На рабочем месте Администратора безопасности могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах в структурных подразделениях, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится через машинные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации.

11.7. При невозможности ликвидации последствий заражения программными вирусами Администратору безопасности необходимо:

11.7.1. сообщить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

11.7.2. заархивировать зараженные файлы с внедренными программными вирусами и направить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

11.7.3. осуществить полную переустановку программного обеспечения на зараженном компьютере.

11.8. 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.

12. Порядок установки и обновления программного обеспечения

12.1. В информационных системах производится установка (инсталляция) только разрешенного Администратором безопасности к использованию в информационной системе программного обеспечения и (или) его компонентов.

12.2. Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов осуществляется только от имени администратора.

12.3. Несанкционированная загрузка программного обеспечения и (или) его компонентов из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) блокируется средствами защиты информации.

12.4. Администратор безопасности обеспечивает периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет разрешения к установке в информационной системе, а также на предмет отсутствия программного обеспечения, запрещенного к установке.

12.5. Администратор безопасности контролирует установку обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

12.6. Администратор безопасности получает из доверенных источников и устанавливает обновления программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

12.7. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

12.8. Контроль установки обновлений проводится с периодичностью, установленной администратором безопасности и фиксируется в соответствующих журналах.

12.9. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

13. Регистрация и реагирование на события безопасности

13.1. В информационной системе осуществляется сбор, запись и хранение информации о событиях безопасности.

13.2. События безопасности, подлежащие регистрации в информационной системе, определяются с учетом способов реализации угроз безопасности. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.

13.3. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.

13.4. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется).

13.5. В информационной системе подлежат регистрации следующие события:

13.5.1. вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;

13.5.2. подключение машинных носителей информации и вывод информации на носители информации;

13.5.3. запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;

13.5.4. попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

13.5.5. попытки удаленного доступа.

13.6. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

13.6.1. возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности;

13.6.2. генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту);

13.6.3. хранение информации о событиях безопасности в течение времени, установленного в соответствии администратором безопасности.

13.7. Администратор безопасности осуществляет мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирует на них:

13.7.1. мониторинг (просмотр и анализ) записей регистрации (аудита) проводится для всех событий, подлежащих регистрации, и с периодичностью, установленной администратором безопасности, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе;

13.7.2. в случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности;

13.7.3. правила и процедуры реагирования на события безопасности них регламентируются в Инструкции по действиям персонала в нештатных ситуациях.

13.8. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти предусматривает:

13.8.1. предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

13.8.2. реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

14. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения и персональных данных

14.1. Администратором безопасности обеспечивается периодическое резервное копирование информации на резервные машинные носители информации с возможностью восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного Администратором безопасности временного интервала, предусматривающее:

14.1.1. резервное копирование информации на резервные машинные носители информации с установленной Администратором безопасности периодичностью;

14.1.2. разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;

14.1.3. регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

14.1.4. принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность;

14.1.5. определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;

14.1.6. восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;

14.1.7. регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

14.1.8. оказание помощи в решении проблем, возникающих при эксплуатации программ архивирования и восстановления информации.

14.2. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники.

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

14.3.1. обязательное хранение всех архивов в защищенном месте;

14.3.2. частота архивации данных зависит от их важности и частоты их изменения;

14.3.3. системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;

14.3.4. данные, которые изменяются очень редко, не имеет смысла архивировать.

14.3.5. восстановление работоспособности программных средств и информационных массивов, в случае утери и повреждения.

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

14.4.1. все файлы операционной системы и установленных приложений. Архивирование системных файлов должно производиться только после установки новых приложений или обновления самой операционной системы;

14.4.2. личные профили пользователей;

14.4.3. папки, содержащие важные документы;

14.4.4. базы данных;

14.4.5. другие файлы и папки, представляющие ценность.

14.5. Организация архивирования и восстановления прикладного программного обеспечения и персональных данных является необходимым элементом защиты информационных ресурсов от их модификации и уничтожения. Организация архивирования и восстановления прикладного программного обеспечения и персональных данных на серверах и рабочих станциях должна, как правило, проводиться по согласованию с Администратором безопасности в нерабочее время, за исключением внештатных ситуаций.

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

14.6.1. системы жизнеобеспечения;

14.6.2. системы обеспечения отказоустойчивости;

14.6.3. системы резервного копирования и хранения данных;

14.6.4. системы контроля физического доступа.

Системы жизнеобеспечения включают:

14.6.5. пожарные сигнализации и системы пожаротушения;

14.6.6. системы вентиляции и кондиционирования;

14.6.7. системы резервного питания.

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

14.8. 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.

14.9. 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:

14.9.1. локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

14.9.2. источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

14.9.3. дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

14.9.4. резервные линии электропитания в пределах комплекса зданий;

14.9.5. аварийные электрогенераторы;

14.9.6. системы обеспечения отказоустойчивости (кластеризация; технология RAID).

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

14.10.1. для обрабатываемых персональных данных – не реже раза в неделю;

14.10.2. для технологической информации – не реже раза в месяц;

14.10.3. 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).

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

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

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

15. Контроль (анализ) защищенности персональных данных

15.1. С целью своевременного выявления и предотвращения утечки персональных данных по техническим каналам, исключения или существенного затруднения несанкционированного доступа к ним и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности или доступности персональных данных, в Организации проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

15.2. Контроль заключается в:

15.2.1. выявлении (поиске), анализе и устранении уязвимостей в информационных системах;

15.2.2. проверке работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

15.2.3. проверке состава технических средств, программного обеспечения и средств защиты информации (проведение инвентаризации);

15.2.4. контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей;

15.2.5. осуществлении размещения устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

15.2.6. проверке выполнения требований нормативных документов по защите персональных данных, а также в оценке их обоснованности и эффективности принятых мер.

15.3. Администратор безопасности осуществляет выявление (поиск), анализ и устранение уязвимостей в информационной системе, включающее:

15.3.1. выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

15.3.2. разработку по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

15.3.3. анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

15.3.4. устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного

обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

15.3.5. информирование пользователей, администраторов, ответственных за организацию обработки персональных данных о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

15.4. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

15.5. Выявление (поиск), анализ и устранение уязвимостей производится на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной администратором безопасности. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

15.6. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

15.7. Администратор безопасности получает из доверенных источников обновления базы признаков уязвимостей.

15.8. Администратор безопасности контролирует работоспособность, параметры настройки и правильности функционирования программного обеспечения и средств защиты информации, включающий:

15.8.1. контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

15.8.2. проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;

15.8.3. контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

15.8.4. восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

15.9. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной администратором безопасности.

15.10. Администратор безопасности контролирует состав технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация), осуществляя:

15.10.1. контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

15.10.2. контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

15.10.3. контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

15.10.4. исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

15.11. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной администратором безопасности.

15.12. Администратор безопасности контролирует правила генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе, осуществляя:

15.12.1. контроль правил генерации и смены паролей пользователей;

15.12.2. контроль заведения и удаления учетных записей пользователей;

15.12.3. контроль реализации правил разграничения доступом;

15.12.4. контроль реализации полномочий пользователей;

15.12.5. контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации;

15.12.6. устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

15.13. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной администратором безопасности.

15.14. Администратор безопасности контролирует осуществление размещения устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

15.15. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

15.16. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

15.17. Итоги контроля Администратор безопасности фиксирует в «Журнал по учету мероприятий по контролю обеспечения защиты персональных данных в ИС».

16. Действия в случае нештатных ситуаций

16.1. Администратором безопасности предусматривается возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

16.2. 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).

16.3. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

16.3.1. восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

16.3.2. восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

16.3.3. возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных администратором безопасности, позволяющих решать задачи по обработке информации.

16.4. Администратором безопасности применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

17. Организация обучения

17.1. Уровень знаний Администратора безопасности должен быть достаточным для выполнения работ по настройке, поддержания в работоспособном состоянии и контроля эффективности системы защиты ПДн.

17.2. Обучение Администратора безопасности включает подготовку по следующим направлениям:

17.2.1. методы и способы противодействия несанкционированному доступу к защищаемой конфиденциальной информации;

17.2.2. методы и способы противодействия утечки информации по каналам побочных электромагнитных излучений и наводок;

17.2.3. методы и способы противодействия вирусным угрозам (использование антивирусного программного обеспечения);

17.2.4. методы и способы обнаружение сетевых вторжений в сегмент локальной вычислительной сети, в котором производится обработка персональных данных;

17.2.5. криптографические методы защиты конфиденциальной информации при ее передаче по открытым каналам связи;

17.2.6. основы законодательства Российской Федерации в области обеспечения безопасности персональных данных в ИС.

17.3. В ходе выполнения своих должностных обязанностей Администратору безопасности необходимо проводить периодический инструктаж пользователей средств вычислительной техники по правилам работы с используемыми средствами и системами защиты информации.

17.4. Инструктажи проводятся в помещениях Организации, непосредственно на рабочих местах пользователей ПЭВМ, обрабатывающих ПДн.

17.5. В ходе инструктажей освещаются следующие вопросы:

17.5.1. правила работы со средствами защиты информации от несанкционированного доступа;

17.5.2. правила работы с персональными идентификаторами;

17.5.3. правила парольной защитой ПЭВМ;

17.5.4. правила работы с антивирусными средствами, в том числе при использовании отчуждаемых (сменных) носителей;

17.5.5. правила работы с криптографическими средствами защиты конфиденциальной информации при ее передаче по открытым каналам связи.

17.6. Помимо периодических инструктажей Администратор безопасности проводит первичный инструктаж вновь допущенных к ПДн сотрудников Организации, по правилам работы с используемыми средствами и системами зашиты информации. Освещаемые вопросы в ходе первичного инструктажа аналогичны вопросам при периодических инструктажах.

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

«01» октября 2021 г.

Приложение 1

Форма

ЖУРНАЛ

учёта списка пользователей ИС

№ п/п	Фамилия И.О.	Номер ПЭВМ	Дата начала допуска к ПДн	Подпись	Дата окончания допуска к ПДн
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.					

Приложение 2

Форма

МАТРИЦА

доступа пользователей к персональным данным

№ п/п	Группа	ФИО сотрудника	Уровень доступа к ПДн
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.			
31.			
32.			
33.			
34.			

Приложение 3

Лист ознакомления

№ п/п	ФИО сотрудника	Дата ознакомления	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.			
31.			
32.			
33.			
34.			
35.			
36.			