**Политика информационной безопасности в ГБУЗ СО «ТГП №2»**

1. ОБЩИЕ ПОЛОЖЕНИЯ
	1. Настоящая политика информационной безопасности (далее - Политика) утверждается главным врачом ГБУЗ СО «ТГП №2» и определяет мероприятия, процедуры и правила по защите информации в информационных системах ГБУЗ СО «ТГП №2».
	2. Положения настоящей Политики распространяются на следующие информационные системы ГБУЗ СО «ТГП №2»:
* ГИС ЕМИАС;
* ИСПДн «1С Бухгалтерия»;
* ИСПДн «1С Бухгалтерия аптека»
* ИСПДн «Кадры государственных учреждений»
* АИС «АСУЛОН»
* ГИС «ОМС»
* ГИС ФРМО
* ГИС ФРМР
* АИС «Смертность»
* Федеральный регистр «Сахарный диабет»
* Федеральный регистр «Переболевших COVID-19»
* Федеральный регистр «Вакцинации от COVID-19»
* Федеральный регистр «Мониторинга здоровья детей сирот»
* Федеральный регисттр СМП и ВМП
* АИС «Поликлиника».
	1. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).
	2. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в ГБУЗ СО «ТГП №2» относятся:
* сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
* сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
* сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
	1. Целями настоящей Политики являются:
* обеспечение конфиденциальности, целостности, доступности защищаемой информации;
* предотвращение утечек защищаемой информации;
* мониторинг событий безопасности и реагирование на инциденты безопасности;
* нейтрализация актуальных угроз безопасности информации;
* выполнение требований действующего законодательства по защите информации.
	1. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.
	2. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:
* Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
* Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
* «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
* «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
* методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
* «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
* «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.
1. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
	1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах ГБУЗ СО «ТГП №2». Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.
	2. Технологический процесс обработки персональных данных в ГБУЗ СО «ТГП №2»:

 Доступ пользователей к работе в ИСПДн

 Доступ пользователей к информационным ресурсам определяется на основании списка постоянных пользователей ИСПДн и перечня защищаемых информационных ресурсов Учреждения

Разграничение прав доступа пользователей к информационным ресурсам и установление полномочий этим пользователям реализуется ИАО средствами ОС и дополнительными средствами СЗИ от НСД.

Вход в систему осуществляется по персональному имени (персональному идентификатору) и паролю конкретного пользователя. При успешном входе в систему пользователь получает права доступа к устройствам, каталогам, файлам и программам, установленные ИПО.

При увольнении пользователя или переходе в другое подразделение, ИАО или ответственный за эксплуатацию ИСПДн на основании приказа, в последний день работы пользователя (или иной день, указанный в приказе), производится удаление учетной записи пользователя и всех его ресурсов (за исключением необходимых для работы других пользователей).

а. Начало сеанса работы.

Перед началом сеанса работы пользователь включает свою рабочую станцию и проходит процедуру аутентификации.

В процессе аутентификации пользователь использует свои личные логин и пароль. Смена личного пароля производится не реже 1 раза в три месяца. Контроль данного процесса осуществляется ИАО.

б. Регистрация пользователей и назначение прав доступа.

Регистрация пользователей и назначение прав доступа производится администратором информационной безопасности на основании заявления «На создание (продление) учетной записи пользователя».

Зарегистрированный пользователь устанавливает свой личный пароль.

Права доступа устанавливаются пользователю средствами ОС в соответствии с разрешительной системой доступа.

Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей ИСПДн Учреждения.

в. Работа с файлами документов, внесение изменений, хранение

Файлы документов разрабатываются на рабочем месте пользователем, зарегистрированным в ИСПДн Учреждения.

Работа пользователя при подготовке файла документа возможна только после успешного прохождения процедуры аутентификации в ИСПДн.

Пользователи имеют право постоянного хранения файлов (архивов файлов) с ПДн на несъемном жестком магнитном диске АРМ, учтенном в Журнале учета машинных носителей. содержащих персональные данные.

Разработка и подготовка к печати документов производится с применением, установленных на рабочей станции, текстовых и табличных редакторов.

 Распечатка документов производится на принтере, размещенном на ОИ и включенном в технический паспорт на этот ОИ.

По окончании сеанса подготовки документа производится его сохранение в виде файла на несъемном жестком магнитном диске АРМ.

В случае отсутствия необходимости дальнейшей работы с документом, впервые набранным с клавиатуры, пользователь может отказаться от сохранения его в виде файла. Также пользователь может отказаться от сохранения внесенных в файл изменений.

Учичтожение файла может быть произведено без распечатки документа, если в документе отпала необходимость.

Удаление данных (файлов) и временных файлов, содержащие ПДн производится штатными средствами ОС.

г. Работа с МНИ

Общие понятия:

Для разработки и хранения файлов с ПДн могут использоваться МНИ, учтенные и разрешгнные к использованию в ИСПДн в установленном порядке, включенные в технический паспорт на этот ОИ.

В качестве МНИ в ИСПДн в ГБУЗ СО «ТГП №2» могут использоваться (разрешены к использованию) следиэщие накопители информации: ортические (лазерные) диски;порту ввода—вывода ПЭВМ).

МНИ при необходимости выдаются каждому пользователю из числа сотрудников, обрабатывающих персональные данные. Выданный носитель предназначен только для хранения файлов подготовленных документов.

Хранение МНИ пользователя:

-Хранение МНИ пользователя должно осуществляться в соответствии с требованиями инструкции по обращению с носителями ПДн.

д. Резервное копирование.

Резервное копирование информационных ресурсов производится ИАО или ответственный за эксплуатацию ИСПДн в соответствии с правами доступа на МНИ, учтенные в порядке, установленным инструкцией по резервному копированию.

Завершение сеанса работы завершении работы пользователь выполняет штатную процедуру завершения работы в Windows, выключает рабочую станцию.

е. Заключительные положения

Всем сотрудникам. допущенным к работе с ПДн, разъясняется ответственность за нарушение поавил получения, обработки, защиты ПДн.

Лица. виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъектов ПДн. несут ответственность в соответствии с действующим законодательством.

1. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ГИС
	1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ГБУЗ СО «ТГП №2», допущенному к работе с ресурсами ГИС присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ГИС.
	2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе.
	3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ГИС запрещено.
	4. Для администратора безопасности ГИС, для системных администраторов ГИС, для удаленных пользователей (пользователей работающих с ресурсами ГИС через внешние телекоммуникационные сети, но являющихся сотрудниками ГБУЗ СО «ТГП №2»), для внешних пользователей ГИС (пользователей, не являющихся сотрудниками ГИС) предусмотрена двухфакторная аутентификация в ГИС. (для ГИС К1: Для всех пользователей ГИС (в том числе для внешних пользователей и удаленных пользователей) предусмотрена двухфакторная аутентификация) Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов: предъявление физического электронного ключа eToken PRO Java 72K (JaCarta, RuToken и тд), и ввод пароля (пин-кода) доступа к памяти электронного ключа. Электронные ключи и пароли доступа выдаются Администратором в соответствии с теми же требованиями и правилами, установленными для выдачи учетных записей и паролей к ним в данном разделе настоящей Политики. Идентификация электронного ключа и считывание аутентификационной информации с него осуществляется с помощью механизмов средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД) КриптоПРО.
	5. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ГИС для сотрудника ГБУЗ СО «ТГП №2», и предоставления ему (или изменения его) прав доступа к ресурсам ГИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:
* содержание запрашиваемых изменений (регистрация нового пользователя ГИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ГИС ранее зарегистрированного пользователя);
* должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
* полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ГИС);
* заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ГИС.
	1. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ГИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:
* положение о разграничении прав доступа в ГИС (при необходимости, Приложение № 2 к настоящей Политике);
* Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами (Приложение № 3 к настоящей Политике).
	1. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и первичный пароль. Дает ознакомиться с инструкцией Пользователя ГИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ГИС. После допуска к работе в ГИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ГИС.
	2. В ГИС для учетных записей Пользователей, процессов, приложений, гостевых и временных учетных записей разрешен только один параллельный сеанс доступа к ресурсам ГИС. Для привилегированных учетных записей (администратор безопасности и системные администраторы) разрешено не более двух параллельных сеансов доступа к ресурсам ГИС с разных устройств. Настройка разрешения параллельных сеансов доступа к ресурсам ГИС осуществляется Администратором путем указания соответствующих параметров в КриптоПРО. Контроль и отображение числа активных одновременных (параллельных) сеансов доступа для каждой учетной записи осуществляется во вкладке «Сессии» сервера безопасности Dallas Lock 8.0-K.
	3. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ГИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ГИС при разборе инцидентов безопасности.
	4. Для проведения временных работ в ГИС сотрудниками сторонних организаций предусмотрена гостевая временная учетная запись «Guest». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.
	5. В качестве модели разграничения доступа к ресурсам ГИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ГИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ГИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.
	6. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ГИС и сопоставляемые им роли приведены в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
	7. Перечень помещений, в которых разрешена работа с ресурсами ГИС, расположены технические средства ГИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
	8. Перечень устройств (стационарных, мобильных, портативных), используемых в ГИС приведен в приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня. Идентификация и аутентификация устройств в ГИС осуществляется по совокупности имени или ID устройства, и MAC-адреса. Идентификация и аутентификация устройств осуществляется с помощью механизмов СЗИ от НСД КриптоПРО. В случае выявления посторонних устройств, Администратор оперативно блокирует доступ неустановленного устройства к ГИС и созывает ГРИИБ, которая в свою очередь устанавливает причины и последствия такого инцидента.
	9. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети ГБУЗ СО «ТГП №2» на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.
	10. Пользователям запрещены любые действия в ГИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ГИС в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в ГИС перечислены в пункте 5.9 инструкции Администратора.
1. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

4.1. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

В информационной системе персональных данных (ИСПДн) должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках ИСПДн, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором персональных данных;

- разрешение передачи информации в ИСПДн только по маршруту, установленному оператором персональных данных;

- изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором персональных данных;

- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором персональных данных.

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИСПДн, а также между ИСПДн или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу персональных данных через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИСПДн и (или) входящие в ИСПДн.

Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

4.2. Требования к усилению УПД.3:

4.2.1 в ИСПДн должно обеспечиваться управление информационными потоками на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации;

4.2.2. в ИСПДн должно обеспечиваться динамическое управление информационными потоками, запрещающее и (или) разрешающее передачу информации на основе анализа изменения текущего состояния ИСПДн или условий ее функционирования;

4.2.3. в ИСПДн должен исключаться обход правил управления информационными потоками за счет преобразования передаваемой информации;

4.2.4. в ИСПДн должен исключаться обход правил управления информационными потоками за счет встраивания одних данных в другие данные информационного потока;

4.2.5. в ИСПДн должен обеспечиваться контроль соединений между техническими средствами (устройствами), используемыми для организации информационных потоков;

4.2.6. в ИСПДн при передаче информации между сегментами ИСПДн и (или) ИСПДн разных уровней защищенности персональных данных должна обеспечиваться однонаправленная передача информации с использованием аппаратных средств;

4.2.7. в ИСПДн должно обеспечиваться управление информационными потоками на основе структуры передаваемых данных (текст, таблицы, видео, аудиоинформация);

4.2.8. в ИСПДн должно обеспечиваться управление информационными потоками на основе используемых сетевых протоколов;

4.2.9. в ИСПДн должно обеспечиваться управление информационными потоками на основе типов (расширений) файлов и (или) имен файлов;

4.2.10. в ИСПДн должна обеспечиваться возможность запрета, разрешения и изменения маршрута передачи информации только администраторами;

4.2.11. в ИСПДн должно обеспечиваться разделение информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации;

4.2.12. в ИСПДн должна обеспечиваться возможность автоматического блокирования передачи информации при выявлении в передаваемой информации вредоносных компьютерных программ;

4.2.13. в ИСПДн должно осуществляться управление информационными потоками при передаче информации между ИСПДн;

4.2.14. в ИСПДн должна обеспечиваться возможность фильтрации информационных потоков на уровне прикладного программного обеспечения (приложений).

4.2.15. в ИСПДн должна осуществляться накопление статистических данных, проверка и фильтрация сетевых пакетов по их содержимому (технология DPI);

4.2.16. наделение трафика конкретными параметрами (в частности включение уведомлений пользователей, исключение или замена элементов трафика) в зависимости от получателя информации.

1. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
	1. В ГИС разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.
	2. Перечень разрешенного программного обеспечения в ГИС определен в Приложении № 7 к настоящей Политике.
	3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС .
	4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.
	5. Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
	6. На серверной части ГИС при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...
	1. На АРМ Пользователей ГИС при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...
	1. На АРМ Администратора ГИС при загрузке операционных систем серверов запускается следующее программное обеспечение:
* MS SQL Server;
* IIS;
* ...
1. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

6.1. ЗНИ.1 УЧЕТ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.1: Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

Учету подлежат:

съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

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.

Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета 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.

Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

Требования к усилению ЗНИ.1:

1) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:

а) информацию о возможности использования машинного носителя информации вне информационной системы;

б) информацию о возможности использования машинного носителя информации за пределами контролируемой зоны (конкретных помещений);

в) атрибуты безопасности, указывающие на возможность использования этих машинных носителей информации для обработки (хранения) соответствующих видов информации;

2) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая неотторгаемую цифровую метку носителя информации для обеспечения возможности распознавания (идентификации) носителя в системах управления доступом;

3) оператором обеспечиваться маркировка машинных носителей информации (технических средств), дополнительно включающая использование механизмов распознавания (идентификации) носителя информации по его уникальным физическим характеристикам.

Содержание базовой меры ЗНИ.1:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.1 | + | + | + | + |
| Усиление ЗНИ.1 |  |  | 1а | 1а, 1б |

6.2. ЗНИ.2 УПРАВЛЕНИЕ ДОСТУПОМ К МАШИННЫМ НОСИТЕЛЯМ ИНФОРМАЦИИ

Требования к реализации ЗНИ.2: Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций);

Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.

 Требования к усилению ЗНИ.2:

1) применение автоматизированной системы контроля физического доступа в помещения, в которых осуществляется хранение машинных носителей информации;

2) опечатывание корпуса средства вычислительной техники, в котором стационарно установлен машинный носитель информации;

3) в информационной системе должно обеспечиваться применение программных (программно-технических) автоматизированных средств управления физическим доступом к машинным носителям информации;

4) контроль физического доступа лиц к машинным носителям информации в соответствии с атрибутами безопасности, установленными для этих носителей.

Содержание базовой меры ЗНИ.2:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.2 | + | + | + | + |
| Усиление ЗНИ.2 |  |  |  |  |

6.3. ЗНИ.3 КОНТРОЛЬ ПЕРЕМЕЩЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

Требования к реализации ЗНИ.3: Оператором должен обеспечиваться контроль перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;

предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);

учет перемещаемых машинных носителей информации в соответствии с ЗНИ.1;

периодическая проверка наличия машинных носителей информации.

Правила и процедуры контроля перемещения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.3:

1) оператором информационной системы определяются задачи (виды деятельности, функции), для решения которых необходимо перемещение машинных носителей информации за пределы контролируемой зоны;

2) применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации, хранимой на носителе, при перемещении машинных носителей информации за пределы контролируемой зоны;

3) оператором определяется должностное лицо, ответственное за перемещение машинных носителей информации;

4) оператором информационной системы осуществляется периодическая проверка машинных носителей информации после их возврата в пределы контролируемой зоны.

Содержание базовой меры ЗНИ.3:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.3 |  |  |  |  |
| Усиление ЗНИ.3 |  |  |  |  |

6.4. ЗНИ.4 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ НЕСАНКЦИОНИРОВАННОГО ОЗНАКОМЛЕНИЯ С СОДЕРЖАНИЕМ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ НА МАШИННЫХ НОСИТЕЛЯХ, И (ИЛИ) ИСПОЛЬЗОВАНИЯ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ИНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Требования к реализации ЗНИ.4: Оператором должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах должно предусматривать:

определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

защита машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.

Правила и процедуры управления, направленные на исключение несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах, регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.4:

1) оператором должны применяться средства контроля съемных машинных носителей информации;

2) оператором должны применяться в соответствии с законодательством Российской Федерации криптографические методы защиты информации, хранящейся на машинных носителях;

3) оператором должен быть определен перечень машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации).

Содержание базовой меры ЗНИ.4:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.4 |  |  |  |  |
| Усиление ЗНИ.4 |  |  |  |  |

6.5. ЗНИ.5 КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ИНТЕРФЕЙСОВ ВВОДА (ВЫВОДА)

Требования к реализации ЗНИ.5: В информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода).

Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:

определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе;

определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);

принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);

контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться:

опечатывание интерфейсов ввода (вывода);

использование механических запирающих устройств;

удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);

применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.5:

1) в информационной системе должна быть обеспечена регистрация использования интерфейсов ввода (вывода) в соответствии с РСБ.3;

2) оператором обеспечивается конструктивное (физическое) исключение из средства вычислительной техники запрещенных к использованию интерфейсов ввода (вывода);

3) оператором информационной системы обеспечивается программное отключение запрещенных к использованию интерфейсов ввода (вывода).

Содержание базовой меры ЗНИ.5:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.5 |  |  | + | + |
| Усиление ЗНИ.5 |  |  |  | 1 |

6.6. ЗНИ.6 КОНТРОЛЬ ВВОДА (ВЫВОДА) ИНФОРМАЦИИ НА МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Требования к реализации ЗНИ.6: В информационной системе должен осуществляться контроль ввода (вывода) информации на машинные носители информации.

Контроль ввода (вывода) информации на машинные носители информации должен предусматривать:

определение оператором типов носителей информации, ввод (вывод) информации на которые подлежит контролю;

определение оператором категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на машинные носители в соответствии с УПД.2;

запрет действий по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации;

регистрация действий пользователей и событий по вводу (выводу) информации на машинные носители информации в соответствии с РСБ.3.

Правила и процедуры контроля ввода (вывода) информации на машинные носители информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.6:

1) в информационной системе должна создаваться копия информации, записываемой пользователями на съемные машинные носители информации (теневое копирование);

2) оператором должны применяться средства контроля подключения съемных машинных носителей информации.

Содержание базовой меры ЗНИ.6:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.6 |  |  |  |  |
| Усиление ЗНИ.6 |  |  |  |  |

6.7. ЗНИ.7 КОНТРОЛЬ ПОДКЛЮЧЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.7: В информационной системе должен обеспечиваться контроль подключения машинных носителей информации.

Контроль подключения машинных носителей информации должен предусматривать:

определение оператором типов носителей информации, подключение которых к информационной системе разрешено в соответствии с УПД.2;

определение оператором категорий пользователей, которым предоставлены полномочия по подключению носителей к информационной системе в соответствии с УПД.2;

запрет подключения носителей информации, подключение которых к информационной системе не разрешено;

регистрация действий пользователей и событий по подключению к информационной системе носителей в соответствии с РСБ.3.

Правила и процедуры контроля подключения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.7:

1) оператором должен обеспечиваться контроль подключения машинных носителей информации с использованием средств контроля подключения съемных машинных носителей информации, позволяющих устанавливать разрешенные и (или) запрещенные типы и (или) конкретные съемные машинные носители информации для различных категорий пользователей;

2) запрет подключения к информационной системе носителей пользователями, не имеющими полномочий на подключение носителей.

Содержание базовой меры ЗНИ.7:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.7 |  |  |  |  |
| Усиление ЗНИ.7 |  |  |  |  |

6.8. ЗНИ.8 УНИЧТОЖЕНИЕ (СТИРАНИЕ) ИНФОРМАЦИИ НА МАШИННЫХ НОСИТЕЛЯХ ПРИ ИХ ПЕРЕДАЧЕ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ, В СТОРОННИЕ ОРГАНИЗАЦИИ ДЛЯ РЕМОНТА ИЛИ УТИЛИЗАЦИИ, А ТАКЖЕ КОНТРОЛЬ УНИЧТОЖЕНИЯ (СТИРАНИЯ)

Требования к реализации ЗНИ.8: Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.

Требования к усилению ЗНИ.8:

1) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;

2) оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации;

3) оператором перед подключением к информационной системе должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, определяемых оператором;

4) оператором должно быть обеспечено уничтожение машинных носителей информации, которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как оптические диски типа CD-R);

5) оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

а) удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

6) перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

в) очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

г) полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

д) размагничивание машинного носителя информации;

е) физическое уничтожение машинного носителя информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое).

Содержание базовой меры ЗНИ.8:

|  |  |
| --- | --- |
| Мера защиты информации | Класс защищенности информационной системы |
| 4 | 3 | 2 | 1 |
| ЗНИ.8 | + | + | + | + |
| Усиление ЗНИ.8 | 5а | 1, 5б | 1, 5в | 1, 2, 3, 5г |

1. РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА И ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ

7.1. УПД.14 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА

Оператором персональных данных должны обеспечиваться регламентация и контроль использования в информационной системе персональных данных (ИСПДн) технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту персональных данных в ИСПДн.

Регламентация и контроль использования технологий беспроводного доступа должны включать:

* ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с [УПД.2](http://fstec21.blogspot.ru/2017/08/implementation-of-rules-of.html);
* предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
* мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа ИСПДн;
* контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИСПДн до начала информационного взаимодействия с ИСПДн.

Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению УПД.14:**

7.1.1. в ИСПДн обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с [ИАФ.2](http://fstec21.blogspot.ru/2017/07/identification-and-authentication.html);

7.1.2. в ИСПДн обеспечивается мониторинг точек беспроводного подключения устройств к ИСПДн на предмет выявления несанкционированного беспроводного подключения устройств;

7.1.3. в ИСПДн исключается возможность изменения пользователем точек беспроводного доступа ИСПДн;

7.1.4. оператором персональных данных одолжен быть предусмотрен запрет беспроводного доступа к ИСПДн из-за пределов контролируемой зоны;

7.1.5. в ИСПДн должен быть запрещен беспроводный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИСПДн и ее системы защиты персональных данных;

7.1.6. в ИСПДн исключается возможность изменения пользователем устройств и настроек беспроводного доступа;

7.1.7. оператором персональных данных обеспечивается определение местонахождения несанкционированного беспроводного устройства;

7.1.8. оператором персональных данных обеспечивается блокирование функционирования несанкционированного беспроводного устройства.

**Содержание базовой меры УПД.14:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| УПД.14 | + | + | + | + |
| Усиление УПД.14 |  | 1 | 1, 3 | 1, 3, 4, 5 |

7.2. ИАФ.2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ УСТРОЙСТВ, В ТОМ ЧИСЛЕ СТАЦИОНАРНЫХ, МОБИЛЬНЫХ И ПОРТАТИВНЫХ

В информационной системе персональных данных (ИСПДн) до начала информационного взаимодействия (передачи персональных данных от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Оператором персональных данных должен быть определен перечень типов устройств, используемых в ИСПДн и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Идентификация устройств в ИСПДн обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, МАС-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в ИСПДн обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению ИАФ.2:**

7.2.1. в ИСПДн должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними:

а) взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства);

б) аутентификация по уникальным встроенным средствам аутентификации.

**Содержание базовой меры ИАФ.2:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| ИАФ.2 |  |  | + | + |
| Усиление ИАФ.2 |  |  |  |  |

7.3. УПД.2 РЕАЛИЗАЦИЯ НЕОБХОДИМЫХ МЕТОДОВ (ДИСКРЕЦИОННЫЙ, МАНДАТНЫЙ, РОЛЕВОЙ ИЛИ ИНОЙ МЕТОД), ТИПОВ (ЧТЕНИЕ, ЗАПИСЬ, ВЫПОЛНЕНИЕ ИЛИ ИНОЙ ТИП) И ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

В информационной системе персональных данных (ИСПДн) для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором персональных данных методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Методы управления доступом реализуются в зависимости от особенностей функционирования ИСПДн, с учетом угроз безопасности персональных данных и должны включать один или комбинацию следующих методов:

* дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
* ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);
* мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа реализуются на основе установленных оператором персональных данных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе 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 персональных данных и иной информации о функционировании системы защиты персональных данных, а также иным объектам доступа.

Правила разграничения доступа регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению УПД.2:**

7.3.1. в ИСПДн правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в ИСПДн;

7.3.2. в ИСПДн правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;

7.3.3. в ИСПДн правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;

7.3.4. в ИСПДн правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением.

**Содержание базовой меры УПД.2:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| УПД.2 | + | + | + | + |
| Усиление УПД.2 |  | 1, 2, 3 | 1, 2, 3 | 1, 2, 3, 4 |

1. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)

8.1. УПД.16 УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ)

Оператором персональных данных должно быть обеспечено управление взаимодействием с внешними информационными системами персональных данных (ИСПДн), включающими ИСПДн и вычислительные ресурсы (мощности) уполномоченных лиц, ИСПДн, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными ИСПДн, информационное взаимодействие с которыми необходимо для функционирования ИСПДн.

Управление взаимодействием с внешними ИСПДН должно включать:

* предоставление доступа к ИСПДн только авторизованным (уполномоченным) пользователям в соответствии с [УПД.2](http://fstec21.blogspot.ru/2017/08/implementation-of-rules-of.html);
* определение типов прикладного программного обеспечения ИСПДн, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних ИСПДн;
* определение системных учетных записей, используемых в рамках данного взаимодействия;
* определение порядка предоставления доступа к ИСПД не авторизованными (уполномоченным) пользователями из внешних ИСПДн;
* определение порядка обработки, хранения и передачи персональных данных с использованием внешних ИСПДн.

Управление взаимодействием с внешними ИСПДн в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации (ЕСИА), созданной в соответствии с постановлением Правительства Российской Федерации от 28.11.2011 N977.

Правила и процедуры управления взаимодействием с внешними ИСПДн регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению УПД.16:**

8.1.1. оператор персональных данных предоставляет доступ к ИСПДн авторизованным (уполномоченным) пользователям внешних ИСПДн или разрешает обработку, хранение и передачу персональных данных с использованием внешней ИСПДн при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней ИСПДн;

б) при наличии подтверждения выполнения во внешней ИСПДн предъявленных к ней требований о защите персональных данных (наличие оценки эффективности (аттестата) соответствия требованиям по безопасности персональных данных).

**Содержание базовой меры УПД.16:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| УПД.16 | + | + | + | + |
| Усиление УПД.16 | 8.1.1а | 8.1.1а, 8.1.1б | 8.1.1а, 8.1.1б | 8.1.1а, 8.1.1б |

1. ПРАВИЛА И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНО ТЕХНИКИ
	1. В ГБУЗ СО «ТГП №2» в качестве средства доверенной загрузки технических средств применяется система ЗСПД
	2. Для работы с ресурсами ГИС выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).
	3. Администратор контролирует работоспособность ЗСПДв соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации.
	4. В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры:
* опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
* устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
* устанавливается усиленный визуальный контроль за техническим средством.
	1. В проектной документации на систему защиты информации в ГИС обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС.
	2. В качестве компенсирующей меры в ГИС применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку.
	3. В качестве компенсирующей меры в ГИС применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода.
	4. В качестве компенсирующей меры в ГИС применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования.
	5. Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации.
1. ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА

10.1. УПД.13 РЕАЛИЗАЦИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА ЧЕРЕЗ ВНЕШНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Оператором персональных данных должна обеспечиваться защита персональных данных при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы персональных данных (ИСПДн) через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

* установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ИСПДн;
* ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с [УПД.2](http://fstec21.blogspot.ru/2017/08/implementation-of-rules-of.html);
* предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
* мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИСПДн;
* контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИСПДн до начала информационного взаимодействия с ИСПДн (передачи персональных данных).

Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению УПД.13:**

10.1.1. в ИСПДн для мониторинга и контроля удаленного доступа должны применяться автоматизированные средства (дополнительные программные или программно-технические средства);

10.1.2. в ИСПДн используется ограниченное (минимально необходимое) количество точек подключения к ИСПДн при организации удаленного доступа к объектам доступа ИСПДн;

10.1.3. в ИСПДн исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИСПДн и ее системы защиты персональных данных;

10.1.4. в ИСПДн при удаленном доступе обеспечивается применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации;

10.1.5. в ИСПДн обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с ИСПДн;

10.1.6. в ИСПДн должен обеспечиваться запрет удаленного доступа с использованием сетевых технологий и протоколов, определенных оператором по результатам анализа защищенности в соответствии с [АНЗ.1](http://fstec21.blogspot.ru/2017/07/detection-vulnerability-analysis.html) как небезопасных.

**Содержание базовой меры УПД.13:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| УПД.13 | + | + | + | + |
| Усиление УПД.13 |  | 10.1.2, 10.1.3 | 10.1.2, 10.1.3, 10.1.5 | 10.1.1, 10.1.2, 10.1.3, 10.1.5 |

1. ПРАВИЛА И ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ (ПРЕДОТВРАЩЕНИЯ) ВТОРЖЕНИЙ

11.1. ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ (СОВ)

|  |  |  |
| --- | --- | --- |
| Условное обозначение и номер меры | Содержание мер по обеспечению безопасности персональных данных | Уровни защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| СОВ.1 | [Обнаружение вторжений](http://fstec21.blogspot.ru/2017/06/intrusion-detection.html) |  |  | +2 | +2 |
| СОВ.2 | [Обновление базы решающих правил](http://fstec21.blogspot.ru/2017/08/updating-decision-rules.html) |  |  | + | +1, 2, 3 |

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.
"цифра" или "цифра""буква" - должны выполняться требования к усилению данной меры защиты персональных данных. Цифры и буквы, не включенные в таблицу и указанные под рубриками "требования к усилению" применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты персональных данных в информационной системе персональных данных соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.

**СОВ.1 Обнаружение вторжений**

Оператором персональных данных должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к персональным данным, специальные воздействия на персональные данные (носители персональных данных) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений.

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы персональных данных (ИСПДн) (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов ИСПДн (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором персональных данных.

Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования ИСПДн.

Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению СОВ.1:**

11.1.1. оператором персональных данных обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) ИСПДн;

11.1.2. в ИСПДн обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах ИСПДн;

11.1.3. обнаружение и реагирование (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) на компьютерные атаки в масштабе времени, близком к реальному;

11.1.4. защита информации, собранной и сгенерированной системой обнаружения вторжений, от несанкционированного доступа, модификации и удаления;

11.1.5. оператором ИСПДн обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах ИСПДн;

11.1.6. оператором ИСПДн обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем.

**Содержание базовой меры СОВ.1:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| СОВ.1 |  |  | + | + |
| Усиление СОВ.1 |  |  | 2 | 2 |

1. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ
	1. В ГБУЗ СО «ТГП №2» в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей.
	2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ГИС производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.
	3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.
	4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
	5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.
	6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя ГБУЗ СО «ТГП №2».
2. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

13.1. АНЗ.2 КОНТРОЛЬ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Оператором персональных данных должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Оператором персональных данных должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

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 персональных данных и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений проводится с периодичностью, установленной оператором персональных данных в организационно-распорядительных документах по защите персональных данных и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с [АВЗ.2](http://fstec21.blogspot.ru/2017/07/updating-database-of-malware-computer.html), баз решающих правил систем обнаружения вторжений в соответствии с [СОВ.2](http://fstec21.blogspot.ru/2017/08/updating-decision-rules.html), баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению АНЗ.2:**

13.1.1 оператором персональных данных должна осуществляться проверка корректности функционирования обновлений в тестовой среде с обязательным оформлением результатов проверки в соответствующем журнале;

13.1.2 оператором персональных данных обеспечивается регламентация и контроль обновлений программного обеспечения базовой системы ввода-вывода (иного микропрограммного обеспечения).

**Содержание базовой меры АНЗ.2:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| АНЗ.2 | + | + | + | + |
| Усиление АНЗ.2 |  |  |  |  |

1. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
	1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.
	2. В случае добавления новых ТС, ПО и СрЗИ в состав ГИС или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.
	3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.
	4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.
	5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.
	6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом главному врачу ГБУЗ СО «ТГП №2», который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.
2. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

15.1. ОЦЛ.1 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В информационной системе персональных данных (ИСПДн) должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

* контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы ИСПДн;
* контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором персональных данных исходя из возможности реализации угроз безопасности персональных данных, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы ИСПДн;
* контроль применения средств разработки и отладки программ в составе программного обеспечения ИСПДн;
* тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с [АНЗ.1](http://fstec21.blogspot.ru/2017/07/detection-vulnerability-analysis.html) и [АНЗ.2](http://fstec21.blogspot.ru/2017/07/to-control-installation-of-software.html);
* обеспечение физической защиты технических средств ИСПДн в соответствии с [ЗТС.2](http://fstec21.blogspot.ru/2017/09/oorganization-controlled-area.html) и [ЗТС.3](http://fstec21.blogspot.ru/2017/07/access-control-technical-means.html).

В случае если функциональные возможности ИСПДн должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором персональных данных обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора персональных данных по защите персональных данных.

**Требования к усилению ОЦЛ.1:**

15.1.1. в ИСПДн контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

15.1.2. в ИСПДн должен обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Российской Федерации, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

15.1.3 оператором персональных данных исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения персональных данных в целях обеспечения целостности программной среды;

15.1.4 оператором персональных данных обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду);

15.1.5 в ИСПДн должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) ИСПДн (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

**Содержание базовой меры ОЦЛ.1:**

|  |  |
| --- | --- |
| Мера защиты персональных данных | Уровень защищенности персональных данных |
| 4 | 3 | 2 | 1 |
| ОЦЛ.1 |  |  | + | + |
| Усиление ОЦЛ.1 |  |  | 15.1.1, 15.1.3 | 15.1.1, 15.1.3 |

1. ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ
	1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.
	2. Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС .
	3. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС .
	4. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.
	5. Нештатными ситуациями являются:
* разглашение информации ограниченного доступа сотрудниками ГБУЗ СО «ТГП №2», имеющими к ней право доступа, в том числе:
	+ разглашение информации лицам, не имеющим права доступа к защищаемой информации;
	+ передача информации по незащищенным каналам связи;
	+ обработка информации на незащищенных технических средствах обработки информации;
	+ опубликование информации в открытой печати и других средствах массовой информации;
	+ передача носителя информации лицу, не имеющему права доступа к ней;
	+ утрата носителя с информацией.
* неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
	+ несанкционированное изменение информации;
	+ несанкционированное копирование информации;
* несанкционированный доступ к защищаемой информации:
	+ несанкционированное подключение технических средств к средствам и системам ГИС ;
	+ использование закладочных устройств;
	+ использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС ;
	+ использование злоумышленником уязвимостей программного обеспечения ГИС;
	+ использование злоумышленником программных закладок;
	+ заражение ГИС злоумышленником программными вирусами;
	+ хищение носителей информации;
	+ нарушение функционирования технических средств обработки информации;
	+ блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
* дефекты, сбои, отказы, аварии технических средств и систем ГИС;
* дефекты, сбои, отказы программного обеспечения ГИС;
* сбои, отказы и аварии систем обеспечения ГИС;
* природные явления, стихийные бедствия:
	+ термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
	+ механические факторы (повреждения зданий, землетрясения и т. д.);
	+ электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).
	1. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.
	2. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.
	3. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.
	4. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
	5. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:
* корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
* предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
* в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.
	1. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:
* Пользователи корректно отключают и обесточивают свои рабочие места;
* системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
* Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
* в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
* в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
* **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.**

Приложение № 1 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

### ЗАЯВКА

**на внесение изменений в списки пользователей
 и наделение пользователей полномочиями доступа к ресурсам ГИС**

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) ГИС

(нужное подчеркнуть)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность с указанием подразделения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)

(нужное подчеркнуть)

для решения задач:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(список задач согласно формуляров задач)
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Начальник | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (наименование заказывающего подразделения) |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(фамилия) |

|  |  |
| --- | --- |
| Согласовано | Администратор безопасности |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(фамилия) |

### ЗАДАНИЕ

**на внесение изменений в списки пользователей ГИС**

|  |  |
| --- | --- |
|  | Администратору безопасности информации\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(фамилия и инициалы исполнителя) |
|  | **Произвести изменения в списках пользователей**  |
|  | Главный врач ГБУЗ СО «ТГП №2»  \_\_\_\_\_\_\_\_\_ Житлов А.Г.«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |
|  |  |

*Обратная сторона заявки*

Присвоено **имя** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

|  |
| --- |
| Наименование задач |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |  |

Администратор безопасности {ФИО Администратора}

Имя учетной записи, персональный идентификатор и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя ГИС ознакомлен

Пользователь

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, фамилия)

«\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

Приложение № 2 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Положение о разграничении прав доступа в ГИС**

 Исходя из характера и режима обработки защищаемой информации в ГИС определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ГИС приведен в таблице.

|  |  |
| --- | --- |
| **Роль** | **Описание параметров доступа к ресурсам ГИС для данной роли** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Приложение № 3 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС**

 Настоящий Перечень устанавливает перечень лиц, должностей и процессов, допущенных к работе с ресурсами ГИС . Для каждого элемента списка в таблице обязательно указываются ФИО (Имя службы или процесса для неодушевленных субъектов доступа), должность (только для одушевленных субъектов доступа), имя присвоенной учетной записи и роль (в соответствии с Положением о разграничении прав доступа в ГИС). Тип и серийный номер выданного идентификатора указываются только при выдаче пользователю электронного ключа. Роспись о получении электронного ключа ставится только при выдаче пользователю такого ключа.

 В настоящем Перечне не отражены вопросы, связанные с использованием средств криптографической защиты информации (СКЗИ). Перечни пользователей СКЗИ, а также иные учетный данные, связанные с СКЗИ приведены в других журналах и перечнях.

| **№ п/п** | **ФИО сотрудника / Имя службы или процесса** | **Должность** | **Имя присвоенной учетной записи** | **Роль** | **Выдан эл. ключ** | **Роспись о получении эл. ключа** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 4 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Перечень помещений, в которых разрешена работа с ресурсами ГИС , в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения**

| **№ п/п** | **Название/номер помещения** | **Техническое средство ГИС** | **Сотрудники, допущенные в помещение** |
| --- | --- | --- | --- |
| **Тип** | **Модель** | **Учетный №****(серийный, инвентарный)** | **Сетевое имя** | **IP-адрес** | **MAC-адрес** | **ФИО** | **Должность** |
|  | Серверная | Сервер | HP xxxxxx | S/N: xxxxxxx | 1c-server | 192.168.116.3 | xx:xx:xx:xx:xx | Иванов Дмитрий Викторович | Специалист по защите информации |
| Коммутатор | Cisco ASA xxxx | Инв.: xxxxxx | - | 192.168.116.100 | xx:xx:xx:xx:xx | Бойков Игорь Александрович | Системный администратор |
| СХД | HP xxxxxx | S/N: xxxxxxx | backup-server | 192.168.116.254 | xx:xx:xx:xx:xx |
| Ноутбук | Acer xxxxxxxx | S/N: xxxxxxx |  | DHCP | xx:xx:xx:xx:xx |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Приложение № 6 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Список разрешающих правил взаимодействия с внешними телекоммуникационными сетями в ГИС**

| **№ п/п** | **IP/URL ресурса или подсеть** | **Обоснование разрешения** | **Правило** | **Время действия правила** | **Учетные записи, устройства, процессы, для которых действует правило** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Приложение № 7 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Список разрешенного программного обеспечения в ГИС**

| **№ п/п** | **Наименование ПО** | **Тип ПО** | **Цель применения ПО в ГИС** | **Место установки компонентов ПО** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение № 8 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Список прикладного программного обеспечения ГИС , доступного пользователям внешней информационной системы Система 1**

| **№ п/п** | **Наименование ПО** | **Тип ПО** | **Цель допуска к ПО внешних пользователей** | **Пользователи внешних систем, допущенный к работе с ПО** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Приложение № 9 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Список пользователей ГИС и внешних пользователей, которым в соответствии с должностными обязанностями предоставлен удаленный доступ к системе**

| **№ п/п** | **ФИО** | **Является ли сотрудником организации** | **Ресурсы, к которым предоставляется удаленный доступ** | **Обязанности, в связи с которыми предоставляется удаленный доступ или основание для предоставления удаленного доступа** | **Учетная запись, от имени которой предоставляется удаленный доступ** | **Время, на которое предоставляется удаленный доступ** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 10 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Порядок резервирования информационных ресурсов в ГИС**

| **№ п/п** | **Наименование информационного ресурса** | **Место размещения ресурса в системе** | **Вид резервного копирования** | **Ответственный за резервное копирование** | **Место хранения резервной копии** | **Частота резервного копирования** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 11 к Политике информационной

безопасности в ГБУЗ СО «ТГП №2»,

утвержденной приказом

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**План обеспечения непрерывности функционирования ГИС**

| **№ п/п** | **Тип нештатной ситуации** | **Критерии нештатной ситуации** | **Кому и в какие сроки докладывается в рабочее время** | **Кому и в какие сроки докладывается в нерабочее время** | **Срок реализации неотложных действий** | **Срок реализации всех необходимых мероприятий** |
| --- | --- | --- | --- | --- | --- | --- |
|  | Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Обнаружение несанкционированно скопированной или измененной конфиденциальной информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | Сразу после получения информации об инциденте | 1 день |
|  | Обнаружение подключения технических средств к средствам и системам объекта информатизации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 3 часа |
|  | Подключение технических средств к средствам и системам ГИС в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | Сразу после получения информации об инциденте | 3 часа |
|  | Обнаружение закладочных устройств |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | Сразу после получения информации об инциденте | 1 день |
|  | Установка закладочных устройств злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование программных закладок внешним нарушителем в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Использование программных закладок внутренним злоумышленником или обнаружение факта использования |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Обнаружение программных вирусов |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 10 минут в рабочее время (1 час в нерабочее) | 12 часов |
|  | Хищение носителя защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 сутки | 3 дня |
|  | Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 10 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 7 дней |
|  | Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Обнаружение произошедшего факта блокировки доступа к защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 20 минут в рабочее время (1 час в нерабочее) | 1 день |
|  | Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации |  | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 2 часа в рабочее время (12 часов в нерабочее) | 1 день |
|  | Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО | Нарушена работа одного пользователя | Администратору сразу после обнаружения инцидента | Администратору в первый рабочий день после инцидента | 20 минут | 2 дня |
| Нарушена работа группы пользователей | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 20 минут | 1 день |
|  | Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС | Сбой ТС и систем ГИС | Администратору сразу после обнаружения инцидента | Администратору сразу после обнаружения инцидента | 1 час | 2 дня |
| Отказ ТС и систем ГИС, затронувший работу группы пользователей | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час в рабочее время (8 часов в нерабочее) | 1 день |
| Отказ ТС и систем ГИС, затронувший работу одного пользователя | Администратору сразу после обнаружения инцидента | Администратору в первый рабочий день после инцидента | 1 час | 2 дня |
| Авария ТС и систем ГИС | Администратору сразу после обнаружения инцидента | Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Сбои, отказы и аварии систем обеспечения ГИС | Сбой систем обеспечения ГИС | Ответственному за материально- техническое обеспечение сразу после инцидента | Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента | 1 час | 1 день |
| Отказ систем обеспечения ГИС, затронувший работу группы пользователей | Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента | Ответственному за материально- техническое обеспечение и Администратору сразу после обнаружения инцидента | 1 час | 1 день |
| Отказ систем обеспечения ГИС, затронувший работу одного пользователя | Ответственному за материально- техническое обеспечение сразу после инцидента | Ответственному за материально- техническое обеспечение в первый рабочий день после инцидента | 1 час | 2 дня |
| Авария систем обеспечения ГИС | Ответственному за материально- техническое обеспечение, Администратору сразу после обнаружения инцидента | Ответственному за материально- техническое обеспечение, Администратору не позднее 8 часов после инцидента | 1 час | 1 день |
|  | Природные явления, стихийные бедствия, несущие угрозу жизни человека |  | Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации | Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации | 10 минут | 30 минут |
|  | Природные явления, стихийные бедствия, не несущие угрозу жизни человека |  | Руководителю, заместителям Руководителя, Администратору  | Руководителю, заместителям Руководителя, Администратору  | 10 минут | 1 час |