

**АДМИНИСТРАЦИЯ**

**ТЕРНЕЙСКОГО МУНИЦИПАЛЬНОГО ОКРУГА**

**ПРИМОРСКОГО КРАЯ**

 **ПОСТАНОВЛЕНИЕ**

|  |  |  |
| --- | --- | --- |
| 13 декабря 2022 года  |  пгт. Терней |  № 1228  |

**Об утверждении политики информационной безопасности**

**в администрации Тернейского муниципального округа**

Руководствуясь [Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051), [от 27.07.2006 N 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046), «требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012 года № 1119, «требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, «Составом и содержанием 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 от 10.07.2014 № 378, методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России 11 февраля 2014 года, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденным приказом ФСБ от 9 февраля 2005 №66, «Инструкцией 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», утвержденной приказом ФАПСИ от 13 июня 2001 №152, администрация Тернейского муниципального округа постановляет:

Руководствуясь [Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051), [от 27.07.2006 N 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046), «требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012 года № 1119, «требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, «Составом и содержанием 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 от 10.07.2014 № 378, методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России 11 февраля 2014 года, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденным приказом ФСБ от 9 февраля 2005 №66, «Инструкцией 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», утвержденной приказом ФАПСИ от 13 июня 2001 №152, администрация Тернейского муниципального округа постановляет:

Руководствуясь [Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051), [от 27.07.2006 N 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046), «требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012 года № 1119, «требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, «Составом и содержанием 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 от 10.07.2014 № 378, методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России 11 февраля 2014 года, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденным приказом ФСБ от 9 февраля 2005 №66, «Инструкцией 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», утвержденной приказом ФАПСИ от 13 июня 2001 №152, администрация Тернейского муниципального округа постановляет:

Руководствуясь [Федеральными законами от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051), [от 27.07.2006 N 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046), «требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012 года № 1119, «требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, «Составом и содержанием 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 от 10.07.2014 № 378, методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России 11 февраля 2014 года, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденным приказом ФСБ от 9 февраля 2005 №66, «Инструкцией 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», утвержденной приказом ФАПСИ от 13 июня 2001 №152, администрация Тернейского муниципального округа постановляет:

Руководствуясь [Федеральными законами от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://docs.cntd.ru/document/901990051), [от 27.07.2006 № 152-ФЗ "О персональных данных"](http://docs.cntd.ru/document/901990046), «требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 01.11.2012 № 1119, «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11.02.2013 № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18.02.2013 № 21, «Составом и содержанием 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 от 10.07.2014 № 378, методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России 11.02.2014, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденным приказом ФСБ от 09.02.2005 № 66, «Инструкцией 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», утвержденной приказом ФАПСИ от 13.06.2001 №152, администрация Тернейского муниципального округа

**ПОСТАНОВЛЯЕТ:**

 1. Утвердить Политику информационной безопасности в администрации Тернейского муниципального округа (прилагается).

2. Рекомендовать руководителям отраслевых (функциональных), территориальных и иных органов администрации Тернейского муниципального округа, руководителям иных органов местного самоуправления в Тернейском муниципальном округе, руководителям муниципальных учреждений, подключенных к корпоративной сети передачи данных, руководствоваться Политикой, утвержденной настоящим постановлением.
 3. Настоящее постановление вступает в силу со дня его принятия.

 4. Признать утратившим силу постановление администрации Тернейского муниципального округа от 27.05.2021 № 461 «Об утверждении политики информационной безопасности в администрации Тернейского муниципального округа» и все изменения к нему.

5. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Тернейского муниципального округа С.Н. Наумкин

|  |
| --- |
| УТВЕРЖДЕНАпостановлением администрации Тернейского муниципального округа от 13.12.2022 № 1228 |

**Политика информационной безопасности в информационных системах класса защищенности «К3», уровней защищенности персональных данных «УЗ-3, УЗ-4» администрации Тернейского муниципального округа Приморского края**

ОГЛАВЛЕНИЕ

[Термины и сокращения 2](#_Toc66909167)

[1 Общие положения 3](#_Toc66909168)

[2 Правила и процедуры идентификации и аутентификации пользователей 5](#_Toc66909169)

[3 Правила и процедуры управления идентификаторами 6](#_Toc66909170)

[4 Правила и процедуры управления средствами аутентификации (аутентификационной информацией) 6](#_Toc66909171)

[5 Правила и процедуры управления учетными записями пользователей 6](#_Toc66909172)

[6 Правила разграничения доступа 8](#_Toc66909173)

[7 Правила и процедуры управления информационными потоками 9](#_Toc66909174)

[8 Правила и процедуры блокирования сеансов доступа 9](#_Toc66909175)

[9 Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации 9](#_Toc66909176)

[10 Правила и процедуры применения удаленного доступа 9](#_Toc66909177)

[11 Правила и процедуры применения беспроводных соединений (технологий беспроводного доступа) 9](#_Toc66909178)

[12 Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание 10](#_Toc66909179)

[13 Правила и процедуры управления взаимодействием с внешними информационными системами 11](#_Toc66909180)

[14 Правила и процедуры доступа к машинным носителям информации 11](#_Toc66909181)

[15 Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации 12](#_Toc66909182)

[16 Правила и процедуры сбора, записи и хранения информации о событиях безопасности 12](#_Toc66909183)

[17 Правила и процедуры реагирования на сбои при регистрации событий безопасности 13](#_Toc66909184)

[18 Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них 13](#_Toc66909185)

[19 Правила и процедуры защиты информации о событиях безопасности 13](#_Toc66909186)

[20 Правила и процедуры антивирусной защиты 13](#_Toc66909187)

[21 Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) 14](#_Toc66909188)

[22 Правила и процедуры выявления, анализа и устранения уязвимостей 15](#_Toc66909189)

[23 Правила и процедуры контроля установки обновлений программного обеспечения 16](#_Toc66909190)

[24 Правила и процедуры восстановления (в том числе планы по действиям персонала, порядок применения компенсирующих мер) 17](#_Toc66909191)

[25 Правила и процедуры контроля и управления физическим доступом 19](#_Toc66909192)

[26 Правила и процедуры защиты мобильных технических средств 20](#_Toc66909193)

[27 Правила и процедуры защиты среды виртуализации 21](#_Toc66909194)

[28 Виды и порядок проведения контроля 22](#_Toc66909195)

[29 Управление конфигурацией аттестованной информационной системы 23](#_Toc66909196)

[30 Порядок внесения изменений 23](#_Toc66909197)

ТЕРМИНЫ И СОКРАЩЕНИЯ

**ИС** – информационная система.

**ИБ** – информационная безопасность.

**СрЗИ** – средство защиты информации.

**СЗИ от НСД** – средство защиты информации от несанкционированного доступа.

**АРМ** – автоматизированное рабочее место пользователя в ИС.

**ТС** – техническое средство.

**АВЗ** – средства антивирусной защиты.

**ОС** – операционная система.

**Оператор** – администрация Тернейского муниципального округа Приморского края.

**Администратор** **безопасности** – администратор безопасности информации в информационной системе, назначенный из числа сотрудников Оператора (структурного подразделения Оператора) информационной системы.

**Системный администратор** – системный администратор в информационной системе, назначенный из числа сотрудников Оператора (структурного подразделения Оператора) информационной системы.

**Администратор виртуальной инфраструктуры** – администратор виртуальной инфраструктуры в информационной системе, назначенный из числа сотрудников Оператора (структурного подразделения Оператора) информационной системы.

**Гипервизор** – программа (программное обеспечение), создающая среду функционирования других программ (в том числе других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

**Гостевая операционная система** – операционная система, установленная на виртуальной машине.

**Рабочий кабинет** – помещение, в котором размещены рабочие станции пользователей информационных систем.

**Серверное помещение** – помещение, в котором размещены технические средства управления информационной системой (сетевое оборудование, серверы, системы бесперебойного питания, аппаратные платформы средств защиты и т.п.)

**СКУД** – система контроля и управления доступом.

**Аутентификационная информация (информация аутентификации)** – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

**Аутентификация** – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

**Идентификатор** – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

**Идентификация** – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

**Объект доступа** – единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

**Субъект доступа** – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
	1. В настоящем документе определяются правила и процедуры эксплуатации системы защиты информации (политика информационной безопасности) в информационных системах класса защищенности «К3», уровней защищенности персональных данных «УЗ-3, УЗ-4», оператором которых является Администрация Тернейского муниципального округа Приморского края.
	2. Настоящий документ включает в себя регламентацию следующих правил и процедур:
		* правила и процедуры идентификации и аутентификации пользователей;
		* правила и процедуры управления идентификаторами;
		* правила и процедуры управления средствами аутентификации (аутентификационной информацией);
		* правила и процедуры управления учетными записями пользователей;
		* правила разграничения доступа;
		* правила и процедуры управления информационными потоками;
		* правила и процедуры блокирования сеансов доступа;
		* правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации;
		* правила и процедуры применения удаленного доступа;
		* правила и процедуры применения беспроводных соединений (технологий беспроводного доступа);
		* правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание;
		* правила и процедуры управления взаимодействием с внешними информационными системами;
		* правила и процедуры доступа к машинным носителям информации;
		* процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации;
		* правила и процедуры сбора, записи и хранения информации о событиях безопасности;
		* правила и процедуры реагирования на сбои при регистрации событий безопасности;
		* правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них;
		* правила и процедуры защиты информации о событиях безопасности;
		* правила и процедуры антивирусной защиты;
		* правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов);
		* правила и процедуры выявления, анализа и устранения уязвимостей;
		* правила и процедуры контроля установки обновлений программного обеспечения;
		* правила и процедуры восстановления (в том числе планы по действиям персонала, порядок применения компенсирующих мер);
		* правила и процедуры контроля и управления физическим доступом;
		* правила и процедуры защиты мобильных технических средств;
		* правила и процедуры защиты среды виртуализации;
		* виды и порядок проведения контроля;
		* управление конфигурацией аттестованной информационной системы.
	3. Разделение полномочий в системе обеспечения информационной безопасности информационных систем Оператора:
		1. Администратор безопасности осуществляет:
		* организационно-методическое обеспечение информационной безопасности в ИС;
		* консультацию системных администраторов и пользователей в вопросах обеспечение информационной безопасности в ИС;
		* контроль настроек средств защиты информации в ИС;
		* организацию периодического контроля обеспечения защиты информации в ИС;
		* ведение организационной и эксплуатационной документации на ИС и СрЗИ в ИС;
		* контроль состояния работоспособности ИС и СрЗИ в ИС.
		1. Системные администраторы осуществляют:
		* настройку системного и программного обеспечения в ИС;
		* техническую поддержку пользователей ИС;
		* администрирование антивирусного программного обеспечения;
		* обновление операционных систем, эксплуатируемых в ИС.

**2.** **ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ**

* 1. С целью соблюдения принципа персональной ответственности за свои действия, каждому сотруднику Оператора, допущенному к работе в ИС, присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.
	2. Идентификация и аутентификация пользователей производится техническими средствами и системами, используя технологии ОС Windows, и сертифицированные ФСТЭК России средства защиты информации, используемые в ИС.
	3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено. Идентификация пользователей осуществляется по уникальным учетным записям, которые однозначно идентифицируют пользователя. В неидентифицируемые учетные записи, такие как "user", "пользователь", "administrator" и т.д., добавляется в их описание фамилия, имя и отчество того пользователя, кому эта учетная запись принадлежит.
	4. В качестве идентификаторов пользователей в ИС используется логин в домене Active Directory, а также локальные учетные записи.
	5. Аутентификация пользователей в ИС производится при помощи пароля, который задается пользователем, по правилам, указанным в документе «Инструкция пользователя в ИС».
	6. В ИС ответственными за создание, присвоение и уничтожение идентификаторов пользователей является Системный администратор, настройки СЗИ от НСД проводит Администратор безопасности информации.
	7. Допускается использование аппаратных идентификаторов пользователей, таких как:
		+ уникальное устройство (iButton, eToken, RuToken, iKey, смарт-карта и др.);
		+ электронная подпись;
		+ совокупность идентификаторов, указанных в пунктах 2.4, 2.7 (двухфакторная аутентификация).
	8. Для каждого идентификатора определяется следующая информация о пользователе: фамилия, имя, отчество пользователя, должность, место работы (для внешних пользователей).
	9. Учет идентификаторов, выданных пользователям, производится:
		+ средствами службы каталогов и средствами защиты информации, для идентификаторов, указанных в п. 2.4;
		+ в документе «Журнал учета машинных носителей информации», для идентификаторов, указанных в п. 2.7, который разрабатывает Администратор безопасности информации.
	10. В качестве усиления процедур аутентификации допускается использование двухфакторной аутентификации.
	11. При вводе пароля не допускается отображение для пользователя действительного значения аутентификационной информации. Вводимые символы пароля отображаются знаком «\*».
	12. В СЗИ от НСД. используемом в ИС, заданы учетные записи пользователей и администраторов, которые имеют доступ к этому АРМ, что предотвращает возможность аутентификации пользователей, не введенных в настройки СЗИ от НСД.
	13. При внесении или изменении пользователя в ИС, Системный администратор вносит необходимые данные в Active Directory, а Администратор безопасности информации изменяет настройки СЗИ от НСД для возможности аутентификации нового пользователя в ОС.
	14. В ИС возможна аутентификация пользователей, не являющихся сотрудниками Оператора. Такими пользователями могут выступать различные организации, привлекаемые на договорной основе, для выполнения необходимых работ. В таком случае, Системным администратором создается временная учетная запись с необходимыми правами доступа для реализации поставленных задач. Работы в ИС, используя эту учетную запись, проводятся под контролем Администратора безопасности информации.
	15. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации. Администратору безопасности информации и Системному администратору разрешается обходить процедуры идентификации и аутентификации при исправлении неполадок в настройках СЗИ и ОС, в целом. В таких случаях, подробные действия Администратора безопасности определены в документе «Инструкция администратора безопасности в ИС» и «Инструкция системного администратора в ИС», соответственно.

**3. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ**

* 1. В ИС ответственным за создание, присвоение и уничтожение идентификаторов пользователей является Системный администратор.
	2. Идентификаторы пользователей выдаются Системным администратором.
	3. Учет идентификаторов, выданных пользователям, производится:
		+ средствами службы каталогов и средствами защиты информации, для идентификаторов, указанных в п. 2.4;
		+ в документе «Журнал учета машинных носителей информации», для идентификаторов, указанных в п. 2.7, который разрабатывает Администратор безопасности информации.
	4. Системный администратор блокирует неиспользуемые идентификаторы пользователей не позднее 90 дней с момента прекращения их использования.
	5. Системный администратор уничтожает учетную запись пользователя при увольнении сотрудника, а также в случае изменений у него фамилии, имени или отчества с созданием нового идентификатора пользователя.
	6. Системный администратор соблюдает правило запрета повторного использования идентификатора в течении не менее одного года после его уничтожения.

**4** **ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ СРЕДСТВАМИ АУТЕНТИФИКАЦИИ (АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИЕЙ)**

* 1. Ответственным за хранение, выдачу, инициализацию, блокирование средств аутентификации в ИС является Системный администратор.
	2. На всех средствах вычислительной техники Системным администратором осуществляется изменение аутентификационной информации (средств аутентификации), заданной их производителями.
	3. Администратором безопасности информации устанавливаются следующие характеристики паролей для ИС:
		+ длина пароля составляет 6 символов.
		+ в числе символов пароля могут присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, &, \*, $, % и т.п.);
		+ минимальное время действия пароля – 1 день;
		+ максимальное время действия пароля – 90 дней;
		+ при смене пароля новое значение отличается от предыдущего не менее чем в четырех позициях;
		+ максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки программно-технического средства или учетной записи пользователя – 5 попыток;
		+ время блокировки программно-технического средства или учетной записи пользователя после превышения количества неуспешных попыток аутентификации (ввода неправильного пароля) – 15 минут.
	4. В случае компрометации или подозрения компрометации паролей, пользователь ИС обязан незамедлительно обратиться к Системному администратору, который в свою очередь осуществляют незамедлительное блокирование скомпрометированных средств аутентификации.
	5. Доступ к администрированию технических средств и систем, содержащим службы каталогов и локальные учетные записи пользователей, предоставлен только Системному администратору.

**5** **ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ**

* 1. Для каждого пользователя ИС определены необходимые права доступа в соответствии с их должностными инструкциями и выполняемыми задачами.
	2. Пользователи ИС имеют возможность работать только с теми средствами и ресурсами ИС, которые необходимы им для выполнения установленных функциональных обязанностей.
	3. Перечень лиц, допущенных к обработке персональных данных, разрабатывается и поддерживается в актуальном состоянии лицом, ответственным за организацию обработки персональных данных.
	4. В ИС ответственным за создание, присвоение и уничтожение идентификаторов пользователей является Системный администратор.
	5. Создание новой учетной записи.
		1. Создание новой учетной записи в ИС осуществляется Системным администратором.
		2. Внутренний пользователь – пользователь, являющийся сотрудником Оператора. Учетная запись внутреннему пользователю создается на основании заявки на имя начальника Системного администратора, подписываемой руководителем структурного подразделения Оператора, в котором числится внутренний пользователь. В качестве внутренних пользователей дополнительно рассматриваются лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с Федеральным законом № 44-ФЗ от 05.04.2013.
		3. Внешний пользователь – пользователь, не являющийся сотрудником Оператора. При наличии доступа внешних пользователей в ИС разрабатываются индивидуальные правила создания учетных записей таких пользователей в организационно-распорядительной документации на ИС.
		4. Присвоение учетной записи производится в технических средствах и системах, используя возможности ОС Windows, и средств защиты информации.
		5. Оператором, при создании новой учетной записи, определяется тип (временная, постоянная) и права учетной записи (администратор, пользователь).
		6. При создании временных учетных записей срок их жизни контролируется вручную Системным администратором.
		7. Администратор безопасности информации ознакомляет всех пользователей ИС с организационно-распорядительной документацией в сфере защиты информации. Результаты ознакомления заносятся в документ «Журнал ознакомления работников с организационно-распорядительной документацией в сфере защиты информации в ИС».
	6. Выдача учетных данных (идентификаторов и аутентификаторов).
		1. Выдача учетных данных внутренним пользователям производится лично в руки субъекту доступа.
		2. При наличии доступа внешних пользователей в ИС разрабатываются индивидуальные правила выдачи учетных записей таких пользователей в организационно-распорядительной документации на ИС.
	7. Управление учетными записями.
		1. Руководитель структурного подразделения, при необходимости внесения изменений сведений о пользователях, их ролях, обязанностях, полномочиях и ограничениях, заблаговременно оповещает лицо, ответственное за создание, присвоение и уничтожение идентификаторов пользователей.
		2. Системный администратор проводит пересмотр (актуализацию) учетных записей и прав доступа не реже одного раза в 90 дней.
		3. В ИС отсутствуют неиспользуемые учетные записи или учетные записи с истекшим сроком действия.

**6** **ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА**

* 1. Существуют следующие методы разграничения прав доступа:
		+ 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.
	2. Методы разграничения доступа в ИС определяются на этапе проектирования ИС или в процессе функционирования ИС Администратором безопасности и фиксируются в организационно-распорядительной документации.
	3. В качестве метода разграничения доступа в ИС используется дискреционный метод разграничения прав доступа.
	4. Для всех технических средств и систем ИС разработаны разрешительные системы (списки) доступа субъектов доступа к объектам доступа (далее – матрица доступа), которые описаны в техническом паспорте на ИС.
	5. В матрице доступа определены права доступа (операции воздействия) субъектов доступа к объектам доступа (полный доступ, чтение, запись, удаление, выполнение и др.), реализуемые в ИС.
	6. Субъектам доступа разрешены только те права доступа (минимальные права), которые им необходимы для выполнения своих служебных обязанностей.

**7** **ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ**

* 1. В информационной системе осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:
	+ фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными Администратором безопасности информации ИС в техническом паспорте на ИС по типу «запрещено все, что не разрешено»;
	+ реализацию правил управления информационными потоками средствами защиты информации, прошедшими оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации;
	+ использование защищенных каналов доступа при передаче информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена).

**8 ПРАВИЛА И ПРОЦЕДУРЫ БЛОКИРОВАНИЯ СЕАНСОВ ДОСТУПА**

* 1. В информационной системе обеспечивается блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в информационной системе или по запросу пользователя.
	2. Параметры блокирования сеансов доступа определяются, модифицируются и регламентируются Администратором безопасности информации.
	3. Администратором безопасности информации настраивается максимальное время бездействия, по истечению которого блокируется текущий сеанс пользователя.
	4. Блокирование сеанса доступа пользователя сохраняется до прохождения им повторной идентификации и аутентификации в ИС.

**9** **ПРАВИЛА И ПРОЦЕДУРЫ ОПРЕДЕЛЕНИЯ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ, РАЗРЕШЕННЫХ ДО ПРОХОЖДЕНИЯ ИМИ ПРОЦЕДУР ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ**

* 1. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации. Администратору безопасности информации и Системному администратору разрешается обходить процедуры идентификации и аутентификации при исправлении неполадок в настройках СЗИ и ОС, в целом. В таких случаях, подробные действия Администратора безопасности определены в документе «Инструкция администратора безопасности в ИС» и «Инструкция системного администратора в ИС», соответственно.
	2. При необходимости, Администратор безопасности информации может разрешить те или иные действия пользователю до прохождения им идентификации и аутентификации в ИС, что Администратор безопасности информации отражает в организационно-распорядительной документации на ИС.

**10** **ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА**

* 1. Под удаленным доступом понимается процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.
	2. В ИС запрещено применение любых видов удаленного доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) субъектов доступа к объектам доступа для всех пользователей, в том числе для привилегированных пользователей.
	3. Оператором, не реже одного раза в полгода, проводится контроль корректного использования удаленного доступа в ИС путем проверки настроек системы защиты информации ИС и ее журналов.

**11** **ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ БЕСПРОВОДНЫХ СОЕДИНЕНИЙ (ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА)**

* 1. В ИС запрещено применять технологии беспроводного доступа для всех пользователей, в том числе для привилегированных пользователей.
	2. Оператором, не реже одного раза в полгода, проводится контроль использования беспроводных соединений в пределах помещений, в которых расположены технические средства ИС. В качестве средств поиска беспроводных сетей допускается использовать общедоступный инструментарий поиска беспроводных сетей.
	3. Запрет использования беспроводных соединений проводится с использованием сертифицированных ФСТЭК России средств защиты информации от несанкционированного доступа, путем исключения средств беспроводной передачи данных из состава основных технических средств и систем ИС и ограничения прав пользователей ИС на установку дополнительного оборудования и программного обеспечения к ним.

**12** **ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ВКЛЮЧАЯ ПРОЦЕДУРЫ ВЫДАЧИ И ВОЗВРАТА МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, А ТАКЖЕ ИХ ПЕРЕДАЧИ НА ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ**

* 1. Мобильными техническими средствами являются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).
	2. В ИС мобильные технические средства допускается использовать только тем субъектам доступа, для которых использование таких мобильных технических средств необходимо для выполнения своих должностных обязанностей.
	3. В ИС разрешено использование только съемных машинных носителей информации. Портативные вычислительные устройства в ИС запрещены.
	4. В ИС отсутствует программное обеспечение, используемое для взаимодействия с мобильными техническими средствами.
	5. Учет выдачи, возврата съемных машинных носителей информации осуществляется в документе «Журнал учета машинных носителей информации», который разрабатывает Администратор безопасности информации.
	6. При передачи съемных машинных носителей информации на техническое обслуживание, производится уничтожение конфиденциальной информации на машинном носителе в составе комиссии путем двукратной записи произвольной информации в высвобождаемую область памяти.
	7. Мониторинг и контроль за использованием мобильных технических средств осуществляет Администратор безопасности информации.
	8. Оператором, не реже одного раза в полгода, проводится контроль использования мобильных технических средств в ИС на предмет выявления и запрета запрещенных (не учтенных) мобильных технических средств.

**13** **ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЕМ С ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ**

* 1. Для ИС определяются требования к подключению внешних информационных систем. В требованиях учитываются:
		+ доступ к внешним информационным системам предоставляется только авторизованным пользователям;
		+ доступ предоставляется к определенным ресурсам в ИС, необходимым для выполнения своих служебных обязанностей;
		+ требования к наличию договора (соглашения) об информационном взаимодействии с оператором внешней информационной системы;
		+ требования к оценке соответствия внешних информационных систем требованиям безопасности информации.
	2. В ИС не используются системные учетные записи для организации взаимодействия подключения к внешним информационным системам.
	3. В ИС отсутствует возможность входящего подключения сторонних организаций к ИС Оператора.
	4. Возможность и описание организации исходящего взаимодействия ИС с информационными системами сторонних организаций отражается в техническом паспорте на ИС.

**14** **ПРАВИЛА И ПРОЦЕДУРЫ ДОСТУПА К МАШИННЫМ НОСИТЕЛЯМ ИНФОРМАЦИИ**

* 1. Машинными носителями информации (далее – МНИ) являются:
		+ 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, стационарно устанавливаемые в корпус средств вычислительной техники (например, накопители на жестких дисках).
	2. К МНИ, используемым в ИС, относятся:
		+ съемные машинные носители информации;
		+ машинные носители информации, стационарно устанавливаемые в корпус средств вычислительной техники.
	3. Принципы учета МНИ.
		1. Учету подлежат все используемые в ИС МНИ, предназначенные для обработки информации ограниченного доступа.
		2. Учет съемных МНИ осуществляется в документе «Журнал учета машинных носителей информации», который разрабатывает Администратор безопасности информации.
		3. Учет МНИ, стационарно устанавливаемые в корпус средств вычислительной техники, осуществляется в составе основных технических средств и систем, учет которых ведется Администратором безопасности информации в техническом паспорте на ИС.
		4. Учет осуществляется по любым идентификационным признакам (заводской номер, инвентаризационный номер, регистрационный номер в журнале учета или совокупность указанных признаков).
		5. Список лиц, которым разрешен доступ к МНИ, представлен в документе «Перечень лиц, имеющих право доступа к машинным носителям информации и в помещения, в которых установлены технические средства ИС».
	4. Выдача МНИ.
		1. Администратором безопасности информации устанавливается перечень лиц (пункт № 14.3.5), имеющих физический доступ к машинным носителям информации.
		2. Физический доступ к машинным носителям информации предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).
		3. Выдача и возврат МНИ сопровождается записью в документе «Журнал учета машинных носителей информации».
	5. Условия, обеспечивающие сохранность съемных и портативных МНИ.
		1. Хранение съемных и портативных МНИ осуществляется в сейфах (шкафах) или надежно запираемых ящиках, оборудованных замками при наличии двух или более дубликатов ключей.
		2. Использование личных МНИ для обработки информации ограниченного доступа запрещается.

**15** **ПРОЦЕДУРЫ УНИЧТОЖЕНИЯ (СТИРАНИЯ) ИНФОРМАЦИИ НА МАШИННЫХ НОСИТЕЛЯХ, А ТАКЖЕ КОНТРОЛЯ УНИЧТОЖЕНИЯ (СТИРАНИЯ) ИНФОРМАЦИИ**

* 1. При передаче МНИ пользователю, который по технологии работы в ИС (служебной необходимости) не имеет права доступа к информации на передаваемых МНИ, а также в сторонние организации для ремонта или утилизации, вся информация, хранящаяся на них, подлежит уничтожению (стиранию).
	2. Уничтожение (стирание) информации с МНИ осуществляется Администратором безопасности информации в составе комиссии путем двукратной записи произвольной информации в высвобождаемую область памяти с помощью встроенных в средства защиты информации от несанкционированного доступа функций, либо иного программного (аппаратного) обеспечения гарантированного уничтожения (стирания) информации. После стирания информации с МНИ производится его форматирование.
	3. Пришедшие в негодность МНИ подлежат уничтожению путем физического (механического) разрушения.
	4. Уничтожение (стирание) МНИ, предназначенных для обработки информации ограниченного доступа, оформляется актом.

**16** **ПРАВИЛА И ПРОЦЕДУРЫ СБОРА, ЗАПИСИ И ХРАНЕНИЯ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ**

* 1. Для ИС определяется перечень событий безопасности, подлежащие регистрации. Перечень определяется на этапе ее проектирования, модифицируются в процессе их использования и регламентируются в организационно-распорядительной документации.
	2. События безопасности, подлежащие регистрации в информационной системе, определяются с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, относятся любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.
	3. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.
	4. Перечень регистрируемых событий безопасности информации описан в техническом паспорте на ИС.
	5. Для журналов событий каждой технологии (сервиса) срок хранения журналов событий определяется Администратором безопасности информации.
	6. Просмотр журналов событий в ИС осуществляется администратором безопасности информации.
	7. Оператором не реже одного раза в квартал, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, обеспечивается пересмотр перечня событий безопасности, подлежащих регистрации.

**17** **ПРАВИЛА И ПРОЦЕДУРЫ РЕАГИРОВАНИЯ НА СБОИ ПРИ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ**

* 1. В информационной системе Администратором безопасности информации осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.
	2. Реагирование на сбои при регистрации событий безопасности предусматривает:
		+ предупреждение (сигнализация, индикация) Администратора безопасности информации о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
		+ реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.
	3. При обнаружении сбоев Администратор безопасности информации:
		+ проводит их устранение в течение 2х рабочих дней;
		+ инициирует служебную проверку по факту сбоев.

**18** **ПРАВИЛА И ПРОЦЕДУРЫ МОНИТОРИНГА РЕЗУЛЬТАТОВ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА НИХ**

* 1. Администратор безопасности информации не реже одного раза в 90 дней осуществляет мониторинг всех событий безопасности, подлежащих регистрации на всех серверах и выборки АРМ пользователей в составе не менее 5% от общего состава компьютеров ИС.
	2. При выявлении признаков инцидентов безопасности в ИС Администратор безопасности информации проводит мероприятия по реагированию на выявленные инциденты безопасности в течение 2х рабочих дней.
	3. Администратор безопасности информации осуществляет планирование проведения подобных мероприятий.

**19** **ПРАВИЛА И ПРОЦЕДУРЫ ЗАЩИТЫ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ**

* 1. В ИС используются следующие методы защиты информации о событиях безопасности:
		+ логическое ограничение доступа к местам хранения журналов событий;
		+ управление журналами событий (доступ к управлению журналами разрешен только привилегированным пользователям ИС).
	2. Оператором, не реже одного раза в два года, в рамках внутреннего контроля, проводится контроль реализации методов защиты информации о событиях безопасности путем проверки настроек системы защиты информации, а также правил разграничения доступа в ИС.

**20** **ПРАВИЛА И ПРОЦЕДУРЫ АНТИВИРУСНОЙ ЗАЩИТЫ**

* 1. Средства антивирусной защиты в ИС могут применяться (исходя из состава ИС):
		+ на автоматизированных рабочих местах;
		+ на серверах;
		+ на периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), где существует техническая возможность;
		+ на мобильных технических средствах;
		+ на иных точках доступа в ИС, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).
	2. В ИС применяются только сертифицированные по требованиям ФСТЭК России средства АВЗ.
	3. Установка, конфигурирование и управление средствами АВЗ осуществляется Системным администратором и Администратором безопасности информации.
	4. Параметры настройки средств антивирусной защиты определяются Администратором безопасности информации.
	5. На АРМ проводятся следующие виды антивирусных проверок:
		+ быстрая проверка – при загрузке операционной системы;
		+ полная проверка – не реже одного раза в неделю;
		+ принудительная проверка – при подключении съемных носителей информации, при загрузке, исполнении, открытии или чтении файлов.
	6. На серверах проводятся следующие виды антивирусных проверок:
		+ быстрая проверка – при загрузке операционной системы;
		+ полная проверка – не реже одного раза в неделю;
		+ принудительная проверка – при подключении съемных носителей информации, при загрузке, исполнении, открытии или чтении файлов.
	7. В периметральных средствах защиты информации проводится проверка в режиме реального времени.
	8. На мобильных технических средствах проводятся следующие виды антивирусных проверок:
		+ быстрая проверка – при загрузке операционной системы;
		+ полная проверка – не реже одного раза в неделю;
		+ принудительная проверка – при подключении съемных носителей информации, при загрузке, исполнении, открытии или чтении файлов.
	9. Доступ к консоли управления антивирусным средством ограничивается паролем с учетом требований парольной защиты в ИС.
	10. Пользователям запрещается отключать средства АВЗ и самостоятельно вносить изменения в их настройки.
	11. Установку парольного доступа к настройкам средств АВЗ производит Системный администратор.
	12. При подключении внешних и съемных носителей информации в ИС проводится автоматическая быстрая проверка на наличие вирусных программ.
	13. Автоматическая проверка объектов (файлов) проводится при загрузке, открытии или исполнении таких файлов.
	14. Мониторинг событий средств АВЗ и реагирование на вирусное заражение осуществляется Администратором безопасности информации с периодичностью не реже одного раза в неделю.
	15. По запросу вышестоящего руководства, Администратор безопасности информации формирует отчет о вирусной активности.
	16. В случае обнаружения вредоносных программ пользователи ИС руководствуются документом «Инструкция пользователя в ИС».
	17. В случае получения информации о фактах заражения ИС Администратор безопасности информации руководствуются документом «Инструкция администратора безопасности информации в ИС».

**21** **ПРАВИЛА И ПРОЦЕДУРЫ ОБНОВЛЕНИЯ БАЗЫ ДАННЫХ ПРИЗНАКОВ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)**

* 1. Обновление сигнатур АВЗ в ИС осуществляется в автоматическом режиме при появлении новых обновлений. Также в ИС присутствует возможность ручного обновления сигнатур.
	2. Ручное обновление сигнатур, а также настройку автоматического обновления производит Системный администратор в ИС.
	3. Источником обновлений являются сервера обновлений производителя средств АВЗ;
	4. Также в качестве источника обновлений может выступать зеркальный сервер, созданный внутри локальной вычислительной сети Оператора.
	5. В ИС исключена возможность получения обновлений сигнатур из не доверенных источников обновлений.
	6. Минимальная периодичность проверки и получения обновлений составляет один раз в сутки.

**22** **ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ**

* 1. Анализ защищенности и поиск уязвимостей ИС организует и проводит комиссия, в состав которой входят Администратор безопасности информации проверяемой информационной системы и назначенный сотрудник Оператора. В качестве инструментальных средств применяются сертифицированные ФСТЭК России средства анализа защищенности (Сканер-ВС, XSpider, RedCheck и пр.).
	2. При выявлении (поиске), анализе и устранении уязвимостей в информационной системе Администратором безопасности информации проводится:
		+ выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
		+ разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
		+ анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
		+ устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
		+ информирование руководителя о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.
	3. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств предпринимаются действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.
	4. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, предоставляемые разработчиком средства анализа защищенности, которое используется для анализа в ИС.
	5. В качестве источников обновления используются доверенные источники обновлений, которые предоставляют разработчики средства анализа защищенности, используемого для анализа в ИС.
	6. На этапе эксплуатации ИС, поиск и анализ уязвимостей проводится не реже одного раза в квартал. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.
	7. Доступ к настройкам средств анализа защищенности ограничивается при помощи парольной защиты, которым владеет только Администратор безопасности информации.
	8. Анализ всех сетевых узлов ИС проводится:
		+ не реже одного раза в квартал;
		+ при внедрении новых узлов и/или технологий в ИС;
		+ при появлении информации о новых уязвимостях.
	9. Анализ защищенности узлов проводится следующими механизмами:
		+ сканер портов;
		+ сканер TCP/UDP-сервисов;
		+ сканер уязвимостей в:
		+ прикладном программном обеспечении;
		+ системном программном обеспечении.
		+ подбор учетных записей в:
		+ протоколах электронной почты (SMTP, POP3 и др.);
		+ службах передачи файлов (NetBIOS/SMB, FTP, HTTP и др.);
		+ протоколах удаленного управления (Telnet, SNMP, MS RDP, SSH, VNC и др.);
		+ базах данных (MS SQL Server, Oracle, Oracle SID/SERVICE\_NAME, MySQL и др.).
	10. По решению Администратора безопасности информации может быть проведено полное «глубокое» сканирование (по всему диапазону портов со всеми включенными механизмами тестов на проникновение).
	11. Сканирование ИС осуществляется изнутри периметра локальной-вычислительной сети (по «частным» IP адресам). Дополнительно, в отношении ИС, может осуществляться сканирование снаружи (из сетей связи общего пользования и сетей международного-информационного обмена).
	12. Перед проведением сканирования Администратор безопасности информации (либо назначенный сотрудник Оператора) осуществляет резервирование сканируемых информационных ресурсов.
	13. Сканирование основных технических средств и систем ИС проводится в моменты их максимальной загруженности (в будние дни, с 9.00, до 18.00, не считая время обеда (с 13.00, до 14.00)).
	14. По результатам каждого сканирования производится отметка в документе «Журнал учета мероприятий по контролю обеспечения защиты информации Тернейского муниципального округа».
	15. Контроль за устранением недостатков осуществляет Администратор безопасности информации.

**23** **ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

* 1. На всех элементах ИС (при технической возможности) обеспечивается запрет установки обновлений СрЗИ от имени непривилегированных пользователей.
	2. Сертифицированные по требованиям безопасности информации СрЗИ обновляются только с доверенных источников обновлений сертифицированной поддержки продуктов.
	3. В ИС запрещается устанавливать настройки обновлений СрЗИ с общедоступных недоверенных источников обновлений.
	4. Доверенным источником обновлений считается:
		+ источник обновлений, который указан в паспорте-формуляре средств защиты информации;
		+ источник обновлений, который установлен по умолчанию при установке СрЗИ с сертифицированного дистрибутива продукта.
	5. Установка обновлений несертифицированных операционных систем, используемых в ИС, проводится в автоматическом режиме с серверов разработчика операционных систем. Возможно получение обновлений с развернутых серверов обновлений Оператора ИС.
	6. При отсутствии технической возможности автоматической установки обновлений несертифицированных операционных систем, используемых в ИС, установка осуществляется в ручном режиме.
	7. Установка обновлений СрЗИ проводится Администратором безопасности информации ИС.
	8. Установка обновлений остального прикладного и системного программного обеспечения, используемого в ИС, проводится Системным администратором ИС или Администратором безопасности информации ИС.
	9. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.
	10. Инструкции по порядку и способам обновления программного обеспечения, включая программное обеспечение средств защиты информации, включены в комплект сопровождающей документации соответствующего программного обеспечения.
	11. После осуществления установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, Администратор безопасности информации обязан удостовериться в положительном результате установки обновлений.
	12. В случае выявления отрицательного результата установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, Администратор безопасности информации обязан инициировать повторную установку обновления соответствующего программного обеспечения, включая обновление программного обеспечения средств защиты информации.
	13. Информация о результате установки обновлений хранится в журналах и отчетах программного обеспечения.
	14. Контроль установки обновлений в ИС проводится с периодичностью не реже одного раза в квартал.

**24** **ПРАВИЛА И ПРОЦЕДУРЫ ВОССТАНОВЛЕНИЯ (В ТОМ ЧИСЛЕ ПЛАНЫ ПО ДЕЙСТВИЯМ ПЕРСОНАЛА, ПОРЯДОК ПРИМЕНЕНИЯ КОМПЕНСИРУЮЩИХ МЕР)**

* 1. В ИС предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.
	2. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:
		+ восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
		+ восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
		+ возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных Оператором, позволяющих решать задачи по обработке информации.
	3. В ИС ответственным за восстановления программного обеспечения является Системный администратор ИС, а также Администратор безопасности информации ИС.
	4. Программное обеспечение ИС, может быть разделено на следующие типы:
		+ системное программное обеспечение;
		+ программное обеспечение общего назначения;
		+ специализированное программное обеспечение;
		+ средства защиты информации.
	5. Носители с системным программным обеспечением и программным обеспечением общего назначения хранятся у Системного администратора.
	6. Носители с программным обеспечением средств защиты информации хранятся у Администратора безопасности информации.
	7. Программное обеспечение может поставляться на магнитных (магнито-оптических, оптических) носителях. Исходный носитель с программным обеспечением хранится в специальном помещении (сейфе), а копии – у Администратора безопасности информации. Администратор безопасности информации не должен допускать несанкционированного копирования носителей с программным обеспечением.
	8. Магнитные носители, предназначенные для длительного хранения информации, периодически проверяются на их пригодность и отсутствие сбойных секторов. При появлении сбойных секторов на машинных носителях информация с этих носителей переносится на исправные.
	9. Восстановление программного обеспечения производиться с их носителей в соответствии с инструкциями производителя.
	10. Проверка работоспособности системы защиты информации после ее восстановления осуществляется внепланово в соответствии с разделом 0. Параметры настройки средств защиты определяются на этапе проектирования ИС или в процессе функционирования ИС Администратором безопасности информации и фиксируются в организационно-распорядительной документации.
	11. В процессе восстановления программного обеспечения осуществляется возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, позволяющих решать задачи по обработке информации.
	12. Оператором применяются компенсирующие меры защиты информации (из методического документа «Меры защиты информации в государственных информационных системах», который утвержден ФСТЭК России от 11 февраля 2014 года) в случаях, когда восстановление работоспособности системы защиты информации невозможно.

**25** **ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ФИЗИЧЕСКИМ ДОСТУПОМ**

* 1. Оператором в ИС обеспечивается контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.
	2. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) Оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками Оператора), а также транспортных, технических и иных материальных средств.
	3. Границы контролируемой зоны устанавливаются приказом об организации контролируемой зоны. Схемы контролируемой зоны фиксируются в техническом паспорте на ИС.
	4. В ИС Оператором обеспечивается контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.
	5. В ИС размещение устройств вывода (отображения, печати) информации исключает возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Устройства вывода (отображения, печати) в рабочих кабинетах размещены так, что возможность несанкционированного просмотра выводимой информации исключена.
	6. Для ИС определяется перечень лиц, имеющих право доступа в помещения, в которых установлены технические средства ИС, в который включены только сотрудники (работники) Оператора.
	7. Право доступа в серверные помещения имеет только Системный администратор. При необходимости, под контролем Системного администратора, доступ в серверные помещения может быть предоставлен другим лицам (организациям, выполняющим различные виды работ по договору, и тд).
	8. Способами физической защиты рабочих кабинетов и серверных кабинетов могут являться (выбор способов физической защиты помещений решается Оператором ИС):
		+ надежно запираемые металлические замки;
		+ обеспечение физической охраны на договорной основе;
		+ охранная сигнализация;
		+ установка СКУД;
		+ видеонаблюдение;
		+ пожарная сигнализация;
		+ система пожаротушения;
		+ система управления микроклиматом;
		+ совокупность вышеуказанных мер.
	9. Проведение ремонтных, наладочных или других работ в рабочих кабинетах и серверном помещении допускается только в присутствии сотрудников, имеющих право самостоятельного доступа в них.
	10. Режим безопасности организуют и обеспечивают сотрудники охраны.
	11. Контроль за организацией режима безопасности в помещениях, в которых расположены технические средства ИС, осуществляет Администратор безопасности информации.
	12. Нахождение лиц в помещениях ИС, не включенных в перечень лиц, имеющих право доступа в помещение, возможно только в сопровождении сотрудника Оператора на время, ограниченное необходимостью решение вопросов, связанных с осуществлением полномочий в рамках договоренности, заключенной с Оператором.
	13. Доступ в помещения, в которых осуществляется обработка защищаемой информации, в нерабочее время возможен только по письменной заявке работника Оператора, согласованной с его непосредственным руководителем.
	14. При возникновении нештатных ситуаций (пожар, затопление):
		+ производится локализация источника опасности своими силами, если это не угрожает жизни и здоровью людей;
		+ оповещается руководитель или его заместитель о возникновении нештатной ситуации;
		+ оповещается администратор безопасности информации в ИС (лицо, исполняющее его обязанности) с целью получения указаний по защите информации при данной ситуации.
	15. При возникновении нештатных ситуаций допускается вскрытие помещений, в которых осуществляется обработка защищаемой информации с целью сведения к минимуму последствий нештатной ситуации.
	16. При вскрытии помещения составляется акт вскрытия помещения, в котором осуществляется обработка защищаемой информации, а также инициируется служебное расследование по поводу причин возникновения нештатной ситуаций, с целью предотвращения ее возникновения в будущем.

**26** **ПРАВИЛА И ПРОЦЕДУРЫ ЗАЩИТЫ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ**

* 1. К мобильным техническим средствам, в рамках настоящего документа, относятся съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители), а также портативные вычислительные устройства и устройства связи с возможностью обработки информации (например, ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).
	2. В ИС разрешено использование только съемных машинных носителей информации. Портативные вычислительные устройства в ИС запрещены.
	3. В качестве мер обеспечения защиты мобильных технических средств реализованы следующие меры:
		+ очистка (удаление), уничтожение съемных машинных носителей информации, в соответствии с разделом 0;
		+ выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);
		+ запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах.

27 **ПРАВИЛА И ПРОЦЕДУРЫ ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ**

* 1. Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).
	2. В качестве компонентов виртуальной инфраструктуры рассматриваются:
	+ серверное оборудование;
	+ аппаратное обеспечение консолей управления;
	+ оборудование хранения данных;
	+ сетевое оборудование;
	+ гипервизор;
	+ хостовая операционная система;
	+ виртуальные машины;
	+ программная среда виртуальных машин (в том числе их операционные системы и программное обеспечение);
	+ виртуальное аппаратное обеспечение;
	+ виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения определенных функций в виртуальной инфраструктуре);
	+ программное обеспечение управления виртуальной инфраструктурой (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки);
	+ служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные);
	+ средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.
	1. В качестве объектов доступа в виртуальной инфраструктуре рассматриваются:
	+ программное обеспечение управления виртуальной инфраструктурой;
	+ гипервизор;
	+ хостовая операционная система;
	+ виртуальные машины;
	+ программная среда виртуальных машин (в том числе их операционные системы и программное обеспечение);
	+ виртуальные контейнеры (зоны);
	+ виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре);
	+ средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.
	1. В ИС оператора не используются технологии виртуализации. В администрации отсутствует необходимость в применении средств защиты (реализации мер защиты) информации для защиты среды виртуализации.

**28** **ВИДЫ И ПОРЯДОК ПРОВЕДЕНИЯ КОНТРОЛЯ**

* 1. Периодический контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе, подразделяется на два вида:
	+ внутренний периодический контроль;
	+ внешний инспекционный контроль.
	1. Внутренний периодический контроль.
		1. Оператор инициирует проведение внутреннего периодического контроля за обеспечением уровня защищенности информации, содержащейся в аттестованной по требованиям безопасности информации ИС с периодичностью не реже чем один раз в два года.
		2. Внутренний периодический контроль проводится Оператором самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.
		3. Для проведения внутреннего периодического контроля, ответственным назначается сотрудник Оператора, имеющий необходимый опыт в сфере информационной безопасности (например, Администратор безопасности информации ИС).
		4. В рамках проведения внутреннего периодического контроля необходимо провести:
	+ анализ защищенности и поиск уязвимостей ОС;
	+ сбор и анализ событий безопасности информации в ИС;
	+ анализ актуальных угроз безопасности информации в ИС и проверка соответствия их угрозам в документе «Модель угроз безопасности информации в ИС»;
	+ проверка актуальности организационно – распорядительной документации на ИС;
	+ контроль настроек, работоспособности и правильного функционирования СрЗИ;
	+ информирование и обучение персонала информационной системы (при необходимости);
	+ соответствие состава ИС с указанным в техническом паспорте;
	+ соответствие состава программного обеспечения ИС с указанным в техническом паспорте;
	+ контроль работоспособности прикладного программного обеспечения, необходимого для работы в ИС;
	+ контроль соответствия контрольных сумм и сроков действия сертификатов соответствия на СрЗИ;
	+ контроль актуальности антивирусных баз данных;
	+ контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе;
	+ анализ защиты среды виртуализации (при использовании в ИС технологий виртуализации).
		1. Контроль работоспособности и правильного функционирования СрЗИ производится с использованием штатных средств тестирования СрЗИ и (или) на тестовых данных, приводящих к известному результату (например, программа telnet – для проверки доступности определенного порта; тест антивирусного ПО EICAR; попытки ввода паролей, не соответствующих требованиям политики безопасности: "111", "qwerty" и т.д.).
		2. Контроль соответствия настроек программного обеспечения и СрЗИ производится по параметрам, установленным в эксплуатационной документации ИС (технический паспорт ИС, акт установки и настройки СрЗИ и пр.).
		3. При несоответствии результатов внутреннего периодического контроля организационно – распорядительной, аттестационной, нормативной документации по защите информации, необходимо провести работы по устранению таких несоответствий.
		4. По результатам контроля защищенности информации разрабатываются следующие документы, которые предоставляются Оператору ИС:
	+ протокол по результатам анализа уязвимостей в ИС;
	+ протокол проведения периодического контроля за обеспечением уровня защищенности информации в ИС;
	+ заключение по результатам проведения периодического контроля за обеспечением уровня защищенности информации в ИС.
	1. Внешний инспекционный контроль.
		1. Внешний инспекционный контроль проводится федеральными органами исполнительной власти, уполномоченными в области защиты информации (ФСБ России, ФСТЭК России, Роскомнадзор, Прокуратура Российской Федерации).
		2. Внешний инспекционный контроль может проводится как плановая проверка, так и внеплановая проверка.

**29** **УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

* 1. Администратор безопасности информации ИС инициирует проведение процедуры оценки эффективности принятых мер защиты информации в виде аттестации ИС.
	2. В аттестате соответствия на ИС указываются условия эксплуатации:
		+ то, что запрещено в процессе эксплуатации ИС;
		+ перечень характеристик, об изменениях которых требуется обязательно извещать организацию, выдавшую аттестат соответствия на ИС.
	3. Соблюдение условий эксплуатации обеспечивается Администратором безопасности информации ИС.
	4. Любые работы, влияющие на условия эксплуатации ИС, указанные в аттестате соответствия, согласовываются с Администратором безопасности информации ИС.
	5. В процессе эксплуатации ИС Администратор безопасности информации ИС:
		+ взаимодействует по вопросам эксплуатации ИС с организацией, выдавшей аттестат соответствия на ИС;
		+ анализирует планируемые работы и принимает решение об их разрешении или запрете, согласно плану мероприятий по защите информации;
		+ ведет учет аттестованных ИС;
		+ организует своевременные контроль эффективности принятых мер, средств защиты информации, периодический контроль и повторную аттестацию ИС (при необходимости).

**30** **ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ**

* 1. Внесение изменений в настоящие правила и процедуры осуществляется при изменении правил и процедур эксплуатации системы защиты информации в информационных системах класса защищенности «К3», уровней защищенности персональных данных «УЗ-3, УЗ-4» администрации Тернейского муниципального округа Приморского края.