Приложение 1
к приказу
от 13 октября 2014 №46-ос

Меры защиты информации, обрабатываемой в РС ЕГИСЗ

Термины и определения

РС ЕГИСЗ (Система) – региональный сегмент единой государственной информационной системы в сфере здравоохранении.

Участники РС ЕГИСЗ (Участники) – субъекты государственной, муниципальной и частной систем здравоохранения Тюменской области, фармацевтические и иные организации, осуществляющие деятельность в сфере охраны здоровья, органы управления здравоохранением Тюменской области, территориальный фонд обязательного медицинского страхования Тюменской области и страховые медицинские организации.

Оператор РС ЕГИСЗ (Оператор) - Государственное казенное учреждение Тюменской области «Центр информационных технологий Тюменской области» (далее – ГКУ ТО «ЦИТТО»), осуществляющее деятельность по эксплуатации РС ЕГИСЗ, в том числе по защите, хранению и администрированию доступа к информации, содержащейся в ее базах данных.

ГАУ ТО «МИАЦ» - участник РС ЕГИСЗ, выполняющий методологические функции по развитию и эксплуатации систем, а также обеспечивающий сопровождение систем статистической отчетности и локальных информационных систем.

Пользователи РС ЕГИСЗ (Пользователи) – работники медицинских организаций государственной, муниципальной и частной систем здравоохранения Тюменской области, сотрудники органов управления здравоохранением, фармацевтических и иных организаций, осуществляющих деятельность в сфере охраны здоровья, специалисты центра телефонного обслуживания Тюменской области, пациенты медицинских организаций государственной, муниципальной и частной систем здравоохранения Тюменской области, участвующие в функционировании РС ЕГИСЗ и/или использующие результаты ее функционирования, а также лица, осуществляющие обработку информации, содержащейся в ее базах данных.

Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

БСВВ – базовая система ввода-вывода.

ОС – операционная система.

ПО РС ЕГИСЗ – программное обеспечение РС ЕГИСЗ.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Государственные информационные системы (ГИС) - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

СЗИ РС ЕГИСЗ – система защиты информации РС ЕГИСЗ.

Администратор [системный, безопасности] - пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) ее системы защиты информации (администратор безопасности) в соответствии с установленной ролью.

Анализ уязвимостей - мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

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).

Базовый набор мер защиты информации - минимальный набор мер защиты информации, установленный для соответствующего класса защищенности информационной системы.

Виртуализация - технология преобразование формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Виртуальная машина - вычислительная система, эмулируемая с помощью технологии виртуализации, в которой установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения.

Внешняя информационная система - информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Внешняя информационно-телекоммуникационная сеть - информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Временный файл - файл, создаваемый операционной системой или иным программным обеспечением для сохранения промежуточных результатов в процессе функционирования или передачи данных другому программному обеспечению.

Гипервизор - программа (программное обеспечение), создающая среду функционирования других программ (в том числе других гипервизоров) за счет 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.

Демилитаризованная зона - экранированный сегмент информационной системы, размещенный на ее внешней границе и выполняющий функции "нейтральной зоны"

(буферной зоны безопасности) между защищаемой информационной системой оператора и внешней информационной системой или информационно-телекоммуникационной сетью.

Доверенная загрузка - загрузка операционной системы средства вычислительной техники с заранее определенных постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации.

Доверенный канал - механизм взаимодействия между средствами защиты информационной системы или между средством защиты информации и программным обеспечением информационной системы.

Доверенный маршрут - механизм взаимодействия между субъектом доступа и средством защиты информации информационной системы.

Доступность информации - свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищенные линии связи - линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность информации).

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.

Инцидент - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент программного обеспечения - составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию.

Компонент информационной системы - часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальность информации - свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Локальный доступ - доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация - аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Мобильный код - несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без

предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

Непривилегированная учетная запись - учетная запись пользователя (процесса, выполняемого от его имени) информационной системы.

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.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Отказ в обслуживании - препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы.

Периметр информационной системы - физическая и (или) логическая граница информационной системы (сегмента информационной системы), в пределах которой оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации.

Потенциал нарушителя - мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

Привилегированная учетная запись - учетная запись администратора информационной системы.

Программная среда - совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач.

Роль - предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Сегмент информационной системы - совокупность нескольких компонентов информационной системы, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач.

Событие безопасности (информационной) - идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

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

Техническое средство - аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Технологии мобильного кода - реализованные в программном обеспечении процессы создания и использования мобильного кода (в частности технологии Java, JavaScript, ActiveX, VBScript).

Удаленный доступ - 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.

Управление доступом - ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Устройство - конструктивно законченный технический элемент, имеющий определенное функциональное назначение в информационной системе.

Уязвимость «нулевого дня» - уязвимость, которая становится известной до момента выпуска разработчиком программного обеспечения информационной системы мер защиты информации по ее устранению, исправлений ошибок или соответствующих обновлений.

Уязвимость информационной системы - недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Хостовая операционная система - операционная система, в среде которой функционирует гипервизор.

Целостность информации - свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

1. Общие положения

1.1. Настоящие Требования о защите информации, содержащейся в РС ЕГИСЗ разработаны на основании:

- Модели нарушителя безопасности информации, обрабатываемой в РС ЕГИСЗ;
- Модели угроз безопасности информации, обрабатываемой в РС ЕГИСЗ;
- Акта определения уровня защищенности ПДн при их обработке в ИСПДн данных «Региональный Сегмент Единой государственной информационной системы в сфере здравоохранения»;
- Акта определения класса защищенности ГИС «Региональный Сегмент Единой государственной информационной системы в сфере здравоохранения»;
- Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методического документа ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

1.2. РС ЕГИСЗ создана Распоряжением Правительства Тюменской области от 19.09.2013 № 1581-рп «О Региональном сегменте Единой государственной информационной системы в сфере здравоохранения».

1.3. Департамент здравоохранения Тюменской области:

- имеет правомочия обладателя информации, содержащейся в РС ЕГИСЗ;
- выполняет функции по координации мероприятий по эксплуатации и развитию РС ЕГИСЗ.

1.4. Департамент информатизации Тюменской области:

- осуществляет мероприятия по эксплуатации и развитию РС ЕГИСЗ;
- определяет оператора РС ЕГИСЗ, информационно-технологической инфраструктуры электронного взаимодействия между Единой государственной информационной системой в сфере здравоохранения и участниками РС ЕГИСЗ – субъектами государственной, муниципальной и частной систем здравоохранения Тюменской области, фармацевтическими и иными организациями, осуществляющими деятельность в сфере охраны здоровья, органами управления здравоохранением Тюменской области, территориальным фондом обязательного медицинского страхования Тюменской области и страховыми медицинскими организациями, информационных систем, осуществляющих сбор, хранение, обработку и предоставление информации об органах, организациях государственной, муниципальной и частной систем здравоохранения и об осуществляемой ими медицинской деятельности.

1.5. Согласно приказа департамента информатизации Тюменской области от 10.09.2013 № 216-од «Об операторе Регионального сегмента Единой государственной информационной системе в сфере здравоохранения» оператором РС ЕГИСЗ является ГКУ ТО «ЦИТТО».

1.6. Формирование требований к защите информации, содержащейся в РС ЕГИСЗ, осуществляется обладателем информации.

2. Меры и средствам защиты информации, применяемым в РС ЕГИСЗ

2.1. В ГИС применяются:

- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 3 класса в случае взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и не ниже 4 класса в случае отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;
- средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Далее приведены меры защиты информации в ИС, применимость их к техническим средствам, расположенным в организации, а также необходимые организационно-распорядительные документы:

Усл. обозн. и № меры	**Меры защиты информации в ИС**	**Техническая реализация**	**Организационное обеспечение**
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	ОС, ПО РС ЕГИСЗ	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными	ОС, ПО РС ЕГИСЗ, StoneGate FireWall	Инструкция по идентификации и

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
	записями пользователей, в том числе внешних пользователей		аутентификации в РС ЕГИСЗ
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	ОС, ПО РС ЕГИСЗ, антивирусное средство защиты	Разрешительная система доступа к РС ЕГИСЗ
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между информационными системами	StoneGate FireWall, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
УПД.4	Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование ИС	ОС, ПО РС ЕГИСЗ	Разрешительная система доступа к РС ЕГИСЗ
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	ОС, ПО РС ЕГИСЗ	Разрешительная система доступа к РС ЕГИСЗ
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к ИС)	ПО РС ЕГИСЗ	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	ОС, ПО РС ЕГИСЗ	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	КриптоПРО, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
УПД.14	Регламентация и контроль использования в ИС технологий беспроводного доступа	ПО РС ЕГИСЗ	Разрешительная система доступа к РС ЕГИСЗ
УПД.15	Регламентация и контроль использования в ИС мобильных технических средств	ОС	Разрешительная система доступа к РС ЕГИСЗ
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	БСВВ	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
III. Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	ОС, Агент StoneGate SSL VPN	Разрешительная система доступа к РС ЕГИСЗ
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	ОС, Агент StoneGate SSL VPN	Разрешительная система доступа к РС ЕГИСЗ
IV. Защита машинных носителей информации (ЗНИ)			
ЗНИ.1	Учет машинных носителей информации	ОС	Журнал учета машинных носителей

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
			персональных данных
ЗНИ.2	Управление доступом к машинным носителям информации	ОС	Разрешительная система доступа к РС ЕГИСЗ
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	ОС	Разрешительная система доступа к РС ЕГИСЗ
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)	ОС	Разрешительная система доступа к РС ЕГИСЗ
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.4	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	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в ИС	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
РСБ.7	Защита информации о событиях безопасности	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Антивирусное средство защиты	Инструкция по антивирусной защите

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
			при работе с РС ЕГИСЗ
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Антивирусное средство защиты	Инструкция по антивирусной защите при работе с РС ЕГИСЗ
VII. Обнаружение вторжений (СОВ)			
СОВ.1	Обнаружение вторжений	Антивирусное средство защиты, StoneGate FireWall, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
СОВ.2	Обновление базы решающих правил	Антивирусное средство защиты, StoneGate FireWall, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей	ОС	Разрешительная система доступа к РС ЕГИСЗ
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	ОС	Разрешительная система доступа к РС ЕГИСЗ, Перечень оборудования, системного и прикладного программного обеспечения, а также применяемых средств защиты информации в РС ЕГИСЗ
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по идентификации и аутентификации в РС ЕГИСЗ
IX. Обеспечение целостности ИС и информации (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	ОС	Инструкция по обеспечению целостности РС ЕГИСЗ и информации
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций		Инструкция по обеспечению целостности РС ЕГИСЗ и информации

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама)	Антивирусное средство защиты	Инструкция по антивирусной защите при работе с РС ЕГИСЗ
X. Обеспечение доступности информации (ОДТ)			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		Инструкция по обеспечению целостности РС ЕГИСЗ и информации
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации		Инструкция по обеспечению целостности РС ЕГИСЗ и информации
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала		Инструкция по обеспечению целостности РС ЕГИСЗ и информации
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации		Инструкция по обеспечению целостности РС ЕГИСЗ и информации
XII. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования		Порядок доступа в помещения, в которых ведется обработка информации в РС ЕГИСЗ
ЗТС.3	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 ИС и помещения и сооружения, в которых они установлены		Порядок доступа в помещения, в которых ведется обработка информации в РС ЕГИСЗ
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		Порядок доступа в помещения, в которых ведется обработка информации в РС ЕГИСЗ
XIII. Защита ИС, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.1	Разделение в ИС функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций ИС	ОС, ПО РС ЕГИСЗ	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.3	Обеспечение защиты информации от	КриптоПРО, StoneGate	Разрешительная

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
	раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	система доступа к РС ЕГИСЗ
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	ОС	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода	ПО РС ЕГИСЗ	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	ОС	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	ОС	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	БСВВ, ОС, ПО РС ЕГИСЗ, антивирусное средство защиты, КриптоПРО, StoneGate FireWall, Агент StoneGate SSL VPN, Сетевое оборудование	Инструкция по обеспечению целостности РС ЕГИСЗ и информации
ЗИС.20	Защита беспроводных соединений, применяемых в ИС		Разрешительная система доступа к РС ЕГИСЗ
ЗИС.22	Защита ИС от угроз безопасности информации, направленных на отказ в обслуживании ИС	StoneGate FireWall	Разрешительная система доступа к РС ЕГИСЗ

Усл. обозн. и № меры	Меры защиты информации в ИС	Техническая реализация	Организационное обеспечение
ЗИС.23	Защита периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	StoneGate FireWall, Сетевое оборудование	Разрешительная система доступа к РС ЕГИСЗ
XIV. Выявление инцидентов и реагирование на них (ИНЦ)			
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них		Разрешительная система доступа к РС ЕГИСЗ
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов		Разрешительная система доступа к РС ЕГИСЗ
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами		Разрешительная система доступа к РС ЕГИСЗ
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		Разрешительная система доступа к РС ЕГИСЗ
ИНЦ.5	Принятие мер по устранению последствий инцидентов		Разрешительная система доступа к РС ЕГИСЗ
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов		Разрешительная система доступа к РС ЕГИСЗ
XV. Управление конфигурацией ИС и СЗПДн (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и СЗПДн		Разрешительная система доступа к РС ЕГИСЗ
УКФ.2	Управление изменениями конфигурации ИС и СЗПДн		Разрешительная система доступа к РС ЕГИСЗ
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации ИС и СЗПДн на обеспечение защиты ПДн и согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности ПДн		Разрешительная система доступа к РС ЕГИСЗ
УКФ.4	Документирование информации (данных) об изменениях в конфигурации ИС и СЗПДн		Разрешительная система доступа к РС ЕГИСЗ

3. Конкретизация мер защиты информации в ИС

Конкретизация мер защиты информации в ИС производится на основании нормативных документов ФСТЭК России.

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)

ИАФ.1 Идентификация и аутентификация пользователей, являющихся работниками оператора

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

К внутренним пользователям в целях настоящего документа относятся должностные лица оператора (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами (инструкциями), утвержденными оператором, и которым в информационной системе присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора и которым в информационной системе также присвоены учетные записи.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации - определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

Усиление ИАФ.1 1) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

2) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

3) в ИС должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов)

ИАФ.2 Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

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

Аутентификация устройств в информационной системе 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 по защите информации.

ИАФ.3 Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

Определено должностное лицо (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;

Формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство

Присвоение идентификатора пользователю и (или) устройству

Предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени

Блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление ИАФ.31) оператором должно быть исключено повторное использование идентификатора пользователя в течение:

а) не менее одного года;

2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования:

а) не более 90 дней;

ИАФ.4 Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

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

выдача средств аутентификации пользователям;

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

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

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

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

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

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

защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление ИАФ.41) в случае использования в ИС механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

в) длина пароля не менее 6 символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

ИАФ.5 Защита обратной связи при вводе аутентификационной информации

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи "система - субъект доступа" в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками "*", "•" или иными знаками.

II. Управление доступом субъектов доступа к объектам доступа (УПД)

УПД.1Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

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

объединение учетных записей в группы (при необходимости);

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

заведение, активация, блокирование и уничтожение учетных записей пользователей;

пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;

порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

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

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление УПД.11) оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей;

2) в ИС должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;

3) в ИС должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:

а) более 90 дней;

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 для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором 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 информационной системы, с учетом угроз безопасности информации 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 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 информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

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

Усиление УПД.21) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему;

2) в ИС правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;

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

УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между информационными системами

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

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

разрешение передачи информации в информационной системе только по маршруту, установленному оператором;

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

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

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами 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 защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

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

УПД.4 Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование ИС

Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с УПД.2.

УПД.5 Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС

Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2.

УПД.6 Ограничение неуспешных попыток входа в информационную систему (доступа к ИС)

В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4.

УПД.10 Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с ИАФ.1.

Правила и процедуры блокирования сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление УПД.101) в ИС обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:

а) до 15 минут;

2) в ИС на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование "хранителя экрана", гашение экрана или иные способы);

УПД.11 Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет

действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.

УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы 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 информационной системы;

ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2;

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 информационной системы;

контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

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

2) в ИС используется ограниченное (минимально необходимое) количество точек подключения к ИС при организации удаленного доступа к объектам доступа ИС;

3) в ИС исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации;

5) в ИС обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой;

УПД.14 Регламентация и контроль использования в ИС технологий беспроводного доступа

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам

доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

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) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с УПД.2;

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 информационной системы;

контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

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

Усиление УПД.141) в ИС обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2;

3) в ИС исключается возможность изменения пользователем точек беспроводного доступа ИС;

УПД.15 Регламентация и контроль использования в ИС мобильных технических средств

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В качестве мобильных технических средств рассматриваются 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).

Регламентация и контроль использования мобильных технических средств должны включать:

установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;

использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30;

ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2;

мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;

запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление УПД.151) оператором обеспечивается запрет использования в ИС, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

2) оператором обеспечивается запрет использования в ИС съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

УПД.17 Обеспечение доверенной загрузки средств вычислительной техники

В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

Доверенная загрузка должна обеспечивать:

блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

контроль доступа пользователей к процессу загрузки операционной системы;

контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление УПД.171) в ИС должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;

III. Ограничение программной среды (ОПС)

ОПС.2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;

настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);

выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или невключение в домен);

контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);

определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке ("белый список"), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке ("черный список"). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

IV. Защита машинных носителей информации (ЗНИ)

ЗНИ.1 Учет машинных носителей информации

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).

Усиление ЗНИ.11) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:

а) информацию о возможности использования машинного носителя информации вне ИС;

ЗНИ.2 Управление доступом к машинным носителям информации

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.

ЗНИ.5 Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации

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.

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)

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.

Усиление ЗНИ.81) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;

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

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

V. Регистрация событий безопасности (РСБ)

РСБ.1 Определение событий безопасности, подлежащих регистрации, и сроков их хранения

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

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

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

В информационной системе как минимум подлежат регистрации следующие события:

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

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

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

попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2.

Усиление РСБ.11) оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

3) оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей;

4) оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства РФ, при этом:

а) осуществляется хранение только записей о выявленных событиях безопасности;

РСБ.2 Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей

информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации, состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.

Усиление РСБ.21) в ИС обеспечивается запись дополнительной информации о событиях безопасности, включающую:

а) полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);

РСБ.3 Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с РСБ.1;

генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2;

хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты

возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1.

Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление РСБ.31) в ИС должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;

РСБ.4 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

В информационной системе должно 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.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

предупреждение (сигнализация, индикация) администраторов 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.

Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

РСБ.5 Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

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

Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации.

РСБ.6 Генерирование временных меток и (или) синхронизация системного времени в ИС

В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

РСБ.7 Защита информации о событиях безопасности

В информационной системе должна обеспечиваться защита информации о событиях безопасности.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление РСБ.71) в ИС обеспечивается резервное копирование записей регистрации (аудита);

VI. Антивирусная защита (АВЗ)

АВЗ.1 Реализация антивирусной защиты

Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

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

установку, конфигурирование и управление средствами антивирусной защиты;

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

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

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

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

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

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление АВЗ.11) в ИС должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;

2) в ИС должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах ИС (серверах, АРМах);

АВЗ.2 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление АВЗ.21) в ИС должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);

VII. Обнаружение вторжений (СОВ)

СОВ.1 Обнаружение вторжений

Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) 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 (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором.

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 информационных систем.

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

Усиление СОВ.11) оператором обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) ИС;

2) в ИС обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах ИС;

СОВ.2 Обновление базы решающих правил

Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

получение из доверенных источников и установку обновлений базы решающих правил;

контроль целостности обновлений базы решающих правил.

Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.

VIII. Контроль (анализ) защищенности информации (АНЗ)

АНЗ.1 Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей

Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

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 должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

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

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором. 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.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования

информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

Правила и процедуры выявления, анализа и устранения уязвимостей регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление АНЗ.11) оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИС на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

2) оператор должен уточнять перечень сканируемых в ИС уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;

4) оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности);

АНЗ.2 Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

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

Оператором 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 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 в организационно-распорядительных документах по защите информации 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, баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2, 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 по защите информации.

АНЗ.3 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

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

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

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

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

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Усиление АНЗ.31) в ИС должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;

АНЗ.4 Контроль состава технических средств, программного обеспечения и средств защиты информации

Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

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

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

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

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

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Усиление АНЗ.41) в ИС должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации;

АНЗ.5 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС

Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;

контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;

контроль реализации правил разграничения доступом в соответствии с УПД.2;

контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5;

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

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

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Усиление АНЗ.51) в ИС должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;

IX. Обеспечение целостности ИС и информации (ОЦЛ)

ОЦЛ.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации

В информационной системе 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 информационной системы;

контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;

контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;

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 и АНЗ.2;

обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3.

В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором 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 по защите информации.

Усиление ОЦЛ.11) в ИС 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;

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

ОЦЛ.3 Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

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

Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

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.

Оператором применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

Правила и процедуры восстановления (в том числе планы по действиям персонала, порядок применения компенсирующих мер) отражаются в организационно-распорядительных документах оператора по защите информации.

ОЦЛ.4 Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама)

Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах,

серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;

фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием "черных" списков (запрещенные отправители) и (или) "белых" списков (разрешенные отправители).

Оператором должно осуществляться обновление базы "черных" ("белых") списков и контроль целостности базы "черных" ("белых") списков.

Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

X. Обеспечение доступности информации (ОДТ)

ОДТ.3 Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия "ответов", визуального контроля, контроля трафика, контроля "поведения" системы или иными методами).

При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.

ОДТ.4 Периодическое резервное копирование информации на резервные машинные носители информации

Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;

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

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

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

Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление ОДТ.41) оператором должна осуществляться с установленной им периодичностью проверка работоспособности средств резервного копирования, средств

хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором);

2) оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне ИС) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию;

ОДТ.5 Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала

Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

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

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

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

Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

ОДТ.7 Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации

Оператором должен осуществляться контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий:

контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);

мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);

мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) услуг по передаче информации.

Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.

XII. Защита технических средств (ЗТС)

ЗТС.2 Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

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.

Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.

Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

ЗТС.3 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 ИС и помещения и сооружения, в которых они установлены

Оператором должны обеспечиваться 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.

Контроль и управление физическим доступом должны предусматривать:

определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации.

ЗТС.4 Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

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

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

XIII. Защита ИС, ее средств, систем связи и передачи данных (ЗИС)

ЗИС.1 Разделение в ИС функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций ИС

В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

3) в ИС должно обеспечиваться выделение АРМ для администраторов безопасности;

ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

ЗИС.5 Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечения, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением.

В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств.

ЗИС.7 Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

При контроле использования технологий мобильного кода должно быть обеспечено:

определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе;

определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода;

регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;

исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки.

Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление ЗИС.71) в ИС должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором;

ЗИС.8 Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. При контроле использования технологий передачи речи должно быть обеспечено:

определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе;

определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями;

реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи;

регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи;

исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование.

Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP).

Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.

ЗИС.9 Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации

Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации. При контроле использования технологий передачи видеоинформации должно быть обеспечено:

определение перечня технологий (сервисов) передачи видеоинформации, разрешенных и (или) запрещенных для использования в информационной системе;

определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями;

реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации;

регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации;

исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование.

Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи.

Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.

ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов

В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа "человек посередине").

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10.

Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).

ЗИС.12 Исключение возможности отрицания пользователем факта отправки информации другому пользователю

Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю.

Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться:

определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);

обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3;

регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.

ЗИС.13 Исключение возможности отрицания пользователем факта получения информации от другого пользователя

Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Для исключения возможности отрицания пользователем факта получения информации должны осуществляться:

определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);

обеспечение целостности полученной информации в соответствии с ЗИС.3;

регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.

ЗИС.15 Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором в соответствии с настоящим методическим документом, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

ЗИС.20 Защита беспроводных соединений, применяемых в ИС

Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе. Защита беспроводных соединений включает:

ограничение на использование в информационной системе беспроводных соединений (в частности 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;

предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам информационной системы;

обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации в соответствии с ИАФ.1, ИАФ.2 и ИАФ.6.

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с УПД.13 и ЗИС.3.

ЗИС.22 Защита ИС от угроз безопасности информации, направленных на отказ в обслуживании ИС

В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.

Оператором должен быть определен перечень угроз (типов угроз) безопасности информации, направленных на отказ в обслуживании.

Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.

ЗИС.23 Защита периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);

обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

Правила и процедуры защиты периметра информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Усиление ЗИС.231) в ИС должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы;

2) в ИС должно быть обеспечено предоставление доступа во внутренние сегменты ИС (демилитаризованную зону) из внешних ИС и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия);

3) оператор должен ограничить количество точек доступа в информационную систему из внешних ИС и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков;

4) оператором в ИС:

а) должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса;

б) должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса;

в) должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов в соответствии с законодательством РФ;

5) в ИС должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа "запрещено все, что не разрешено");

XIV. Выявление инцидентов и реагирование на них (ИНЦ)

ИНЦ.1 Определение лиц, ответственных за выявление инцидентов и реагирование на них

ИНЦ.2 Обнаружение, идентификация и регистрация инцидентов

ИНЦ.3 Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами

ИНЦ.4 Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий

ИНЦ.5 Принятие мер по устранению последствий инцидентов

ИНЦ.6 Планирование и принятие мер по предотвращению повторного возникновения инцидентов

XV. Управление конфигурацией ИС и СЗПДн (УКФ)

УКФ.1 Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и СЗПДн

УКФ.2 Управление изменениями конфигурации ИС и СЗПДн

УКФ.3 Анализ потенциального воздействия планируемых изменений в конфигурации ИС и СЗПДн на обеспечение защиты ПДн и согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности ПДн

УКФ.4 Документирование информации (данных) об изменениях в конфигурации ИС и СЗПДн