|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Условное обозначение и номер меры или документ** | | **Меры защиты информации в информационных системах** | | **Приказ  № 21  ФСТЭК России[[1]](#footnote-1)**  **(1 уровень)** | | **Приказ  № 17  ФСТЭК России[[2]](#footnote-2)**  **(2 класс)** | **Адаптация  с учетом особенностей ИС[[3]](#footnote-3)** | **Уточнение с учетом модели угроз[[4]](#footnote-4)** | **Дополнение с учетом законодательства[[5]](#footnote-5)** | **Итог[[6]](#footnote-6)** |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | | | | | | |
| ИАФ.1 | | Идентификация и аутентификация пользователей, являющихся работниками оператора | | + | | + |  |  |  |  |
| ИАФ.1  (усил. 1а) | | В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов) с использованием сети связи общего пользования, в том числе сети Интернет | | - | | + |  |  |  |  |
| ИАФ.1  (усил. 2а) | | В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей) с использованием сети связи общего пользования, в том числе сети Интернет | | - | | + |  |  |  |  |
| ИАФ.1  (усил. 3) | | В информационной системе 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 | | + | | + |  |  |  |  |
| ИАФ.3 | | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | | + | | + |  |  |  |  |
| ИАФ.3  (усил. 1а) | | Оператором должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года | | - | | + |  |  |  |  |
| ИАФ.3  (усил. 2а) | | Оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования 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 | | + | | + |  |  |  |  |
| ИАФ.4  (усил. 1в) | | В случае использования в информационной системе 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: длина пароля не менее шести 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 | | + | | + |  |  |  |  |
| ИАФ.6 | | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | | + | | + |  |  |  |  |
| ИАФ.7 | | Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа | | - | | - |  |  |  |  |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | | | | | | |
| УПД.1 | | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | | + | | + |  |  |  |  |
| УПД.1  (усил. 1) | | Оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей | | - | | + |  |  |  |  |
| УПД.1  (усил. 2) | | В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования | | - | | + |  |  |  |  |
| УПД.1  (усил. 3а) | | В информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования 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 | | + | | + |  |  |  |  |
| УПД.2  (усил. 1) | | В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему | | - | | + |  |  |  |  |
| УПД.2  (усил. 2) | | В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам | | - | | + |  |  |  |  |
| УПД.2  (усил. 3) | | В информационной системе 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 информационной системы, а также между информационными системами | | + | | + |  |  |  |  |
| УПД.4 | | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | | + | | + |  |  |  |  |
| УПД.5 | | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | | + | | + |  |  |  |  |
| УПД.6 | | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | | + | | + |  |  |  |  |
| УПД.7 | | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения установленных оператором правил обработки информации | | - | | - |  |  |  |  |
| УПД.8 | | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему | | - | | - |  |  |  |  |
| УПД.9 | | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы | | - | | - |  |  |  |  |
| УПД.10 | | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | | + | | + |  |  |  |  |
| УПД.10  (усил. 1а) | | В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя: до 15 минут | | - | | + |  |  |  |  |
| УПД.10  (усил. 2) | | В информационной системе 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 | | + | | + |  |  |  |  |
| УПД.12 | | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки | | - | | - |  |  |  |  |
| УПД.13 | | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | | + | | + |  |  |  |  |
| УПД.13  (усил. 2) | | В информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы | | - | | + |  |  |  |  |
| УПД.13  (усил. 3) | | В информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации | | - | | + |  |  |  |  |
| УПД.13  (усил. 5) | | В информационной системе 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 информационной системе технологий беспроводного доступа | | + | | + |  |  |  |  |
| УПД.14  (усил. 1) | | В информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2 | | - | | + |  |  |  |  |
| УПД.14  (усил. 3) | | В информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы | | - | | + |  |  |  |  |
| УПД.15 | | Регламентация и контроль использования в информационной системе мобильных технических средств | | + | | + |  |  |  |  |
| УПД.15  (усил. 1) | | Оператором обеспечивается запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации | | - | | + |  |  |  |  |
| УПД.15  (усил. 2) | | Оператором обеспечивается запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации) | | - | | + |  |  |  |  |
| УПД.16 | | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | | + | | + |  |  |  |  |
| УПД.16  (усил. 1а) | | Оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий: при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы | | - | | + |  |  |  |  |
| УПД.16  (усил. 1б) | | Оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий: при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения) | | - | | + |  |  |  |  |
| УПД.17 | | Обеспечение доверенной загрузки средств вычислительной техники | | + | | + |  |  |  |  |
| УПД.17  (усил. 1) | | В информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения | | - | | + |  |  |  |  |
| III. Ограничение программной среды (ОПС) | | | | | | | | | | |
| ОПС.1 | | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения | | - | | - |  |  |  |  |
| 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 | | + | | + |  |  |  |  |
| ОПС.3 | | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | | + | | + |  |  |  |  |
| ОПС.4 | | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов | | - | | - |  |  |  |  |
| IV. Защита машинных носителей информации (ЗНИ) | | | | | | | | | | |
| ЗНИ.1 | | Учет машинных носителей информации | | + | | + |  |  |  |  |
| ЗНИ.1  (усил. 1а) | | Оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая: информацию о возможности использования машинного носителя информации вне информационной системы | | - | | + |  |  |  |  |
| ЗНИ.2 | | Управление доступом к машинным носителям информации | | + | | + |  |  |  |  |
| ЗНИ.3 | | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | | - | | - |  |  |  |  |
| ЗНИ.4 | | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящихся на машинных носителях, и (или) использования носителей информации в иных информационных системах | | - | | - |  |  |  |  |
| ЗНИ.5 | | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации | | - | | + |  |  |  |  |
| ЗНИ.6 | | Контроль ввода (вывода) информации на машинные носители информации | | - | | - |  |  |  |  |
| ЗНИ.7 | | Контроль подключения машинных носителей информации | | - | | - |  |  |  |  |
| ЗНИ.8 | | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | | + | | + |  |  |  |  |
| ЗНИ.8  (усил. 1) | | Оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации | | - | | + |  |  |  |  |
| ЗНИ.8  (усил. 5в) | | Оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: 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 | | + | | + |  |  |  |  |
| РСБ.1  (усил. 1) | | 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 информационной системе | | - | | + |  |  |  |  |
| РСБ.1  (усил. 3) | | Оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей | | - | | + |  |  |  |  |
| РСБ.1  (усил. 4а) | | Оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом: осуществляется хранение только записей о выявленных событиях безопасности | | - | | + |  |  |  |  |
| РСБ.2 | | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | | + | | + |  |  |  |  |
| РСБ.2  (усил. 1а) | | В информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую: полнотекстовую запись привилегированных команд (команд, управляющих системными функциями) | | - | | + |  |  |  |  |
| РСБ.3 | | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | | + | | + |  |  |  |  |
| РСБ.3  (усил. 1) | | В информационной системе 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 | | - | | + |  |  |  |  |
| РСБ.5 | | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | | + | | + |  |  |  |  |
| РСБ.6 | | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | | - | | + |  |  |  |  |
| РСБ.7 | | Защита информации о событиях безопасности | | + | | + |  |  |  |  |
| РСБ.7  (усил. 1) | | В информационной системе обеспечивается резервное копирование записей регистрации (аудита) | | - | | + |  |  |  |  |
| РСБ.8 | | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе | | - | | - |  |  |  |  |
| VI. Антивирусная защита (АВЗ) | | | | | | | | | | |
| АВЗ.1 | | Реализация антивирусной защиты | | + | | + |  |  |  |  |
| АВЗ.1  (усил. 1) | | В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности | | - | | + |  |  |  |  |
| АВЗ.1  (усил. 2) | | В информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах) | | - | | + |  |  |  |  |
| АВЗ.2 | | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | | + | | + |  |  |  |  |
| АВЗ.2  (усил. 1) | | В информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов) | | - | | + |  |  |  |  |
| VII. Обнаружение вторжений (СОВ) | | | | | | | | | | |
| СОВ.1 | | Обнаружение вторжений | | + | | + |  |  |  |  |
| СОВ.1  (усил. 2) | | В информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы | | - | | + |  |  |  |  |
| СОВ.2 | | Обновление базы решающих правил | | + | | + |  |  |  |  |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | | | | | | | | | |
| АНЗ.1 | | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | | + | | + |  |  |  |  |
| АНЗ.1  (усил. 1) | | 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 информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей | | - | | + |  |  |  |  |
| АНЗ.1  (усил. 2) | | Оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях | | - | | + |  |  |  |  |
| АНЗ.1  (усил. 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 | | + | | + |  |  |  |  |
| АНЗ.3 | | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | | + | | + |  |  |  |  |
| АНЗ.3  (усил. 1) | | В информационной системе 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 | | + | | + |  |  |  |  |
| АНЗ.4  (усил. 1) | | В информационной системе 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 доступа, полномочий пользователей в информационной системе | | + | | + |  |  |  |  |
| АНЗ.5  (усил. 1) | | В информационной системе 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 информационной системы и информации (ОЦЛ) | | | | | | | | | | |
| ОЦЛ.1 | | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | | + | | + |  |  |  |  |
| ОЦЛ.1  (усил. 1) | | В информационной системе 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 | | - | | + |  |  |  |  |
| ОЦЛ.1  (усил. 3) | | Оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды | | - | | + |  |  |  |  |
| ОЦЛ.2 | | Контроль целостности информации, содержащейся в базах данных информационной системы | | - | | - |  |  |  |  |
| ОЦЛ.3 | | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | | - | | + |  |  |  |  |
| ОЦЛ.4 | | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | | + | | + |  |  |  |  |
| ОЦЛ.5 | | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы | | - | | - |  |  |  |  |
| ОЦЛ.6 | | Ограничение прав пользователей по вводу информации в информационную систему | | - | | - |  |  |  |  |
| ОЦЛ.7 | | Контроль точности, полноты и правильности данных, вводимых в информационную систему | | - | | - |  |  |  |  |
| ОЦЛ.8 | | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | | - | | - |  |  |  |  |
| X. Обеспечение доступности персональных данных (ОДТ) | | | | | | | | | | |
| ОДТ.1 | | Использование отказоустойчивых технических средств | | - | | - |  |  |  |  |
| ОДТ.2 | | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | | - | | - |  |  |  |  |
| ОДТ.3 | | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | | + | | + |  |  |  |  |
| ОДТ.4 | | Периодическое резервное копирование информации на резервные машинные носители информации | | + | | + |  |  |  |  |
| ОДТ.4  (усил. 1) | | 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) | | - | | + |  |  |  |  |
| ОДТ.4  (усил. 2) | | Оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) 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 | | + | | + |  |  |  |  |
| ОДТ.6 | | Кластеризация информационной системы и (или) ее сегментов | | - | | - |  |  |  |  |
| ОДТ.7 | | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации | | - | | + |  |  |  |  |
| XI. Защита среды виртуализации (ЗСВ) | | | | | | | | | | |
| ЗСВ.1 | | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | | + | | + |  |  |  |  |
| ЗСВ.1  (усил. 1) | | В информационной системе должны обеспечиваться взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе | | - | | + |  |  |  |  |
| ЗСВ.2 | | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | | + | | + |  |  |  |  |
| ЗСВ.2  (усил. 1) | | В информационной системе должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры | | - | | + |  |  |  |  |
| ЗСВ.2  (усил. 2) | | В информационной системе должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры | | - | | + |  |  |  |  |
| ЗСВ.3 | | Регистрация событий безопасности в виртуальной инфраструктуре | | + | | + |  |  |  |  |
| ЗСВ.4 | | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | | - | | + |  |  |  |  |
| ЗСВ.5 | | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией | | - | | - |  |  |  |  |
| ЗСВ.6 | | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | | + | | + |  |  |  |  |
| ЗСВ.6  (усил. 1) | | Оператором должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных) | | - | | + |  |  |  |  |
| ЗСВ.7 | | Контроль целостности виртуальной инфраструктуры и ее конфигураций | | + | | + |  |  |  |  |
| ЗСВ.7  (усил. 3) | | В информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры | | - | | + |  |  |  |  |
| ЗСВ.8 | | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | | + | | + |  |  |  |  |
| ЗСВ.9 | | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | | + | | + |  |  |  |  |
| ЗСВ.9  (усил. 1) | | В информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты | | - | | + |  |  |  |  |
| ЗСВ.10 | | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | | + | | + |  |  |  |  |
| XII. Защита технических средств (ЗТС) | | | | | | | | | | |
| ЗТС.1 | | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | | - | | - |  |  |  |  |
| ЗТС.2 | | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | | - | | + |  |  |  |  |
| 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 информационной системы и помещения и сооружения, в которых они установлены | | + | | + |  |  |  |  |
| ЗТС.4 | | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | | + | | + |  |  |  |  |
| ЗТС.5 | | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | | - | | - |  |  |  |  |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | | | | | | | | |
| ЗИС.1 | | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы | | + | | + |  |  |  |  |
| ЗИС.1  (усил. 3) | | В информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности | | - | | + |  |  |  |  |
| ЗИС.2 | | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | | - | | - |  |  |  |  |
| ЗИС.3 | | Обеспечение защиты персональных данных 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 | | + | | + |  |  |  |  |
| ЗИС.4 | | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | | - | | - |  |  |  |  |
| ЗИС.5 | | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | | - | | + |  |  |  |  |
| ЗИС.5  (усил. 1) | | В информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны) | | - | | + |  |  |  |  |
| ЗИС.6 | | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами | | - | | - |  |  |  |  |
| 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 | | - | | + |  |  |  |  |
| ЗИС.7  (усил. 1) | | В информационной системе 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 | | - | | + |  |  |  |  |
| 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 | | - | | + |  |  |  |  |
| ЗИС.10 | | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | | - | | - |  |  |  |  |
| ЗИС.11 | | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | | + | | + |  |  |  |  |
| ЗИС.12 | | Исключение возможности отрицания пользователем факта отправки информации другому пользователю | | - | | + |  |  |  |  |
| ЗИС.13 | | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | | - | | + |  |  |  |  |
| ЗИС.14 | | Использование устройств терминального доступа для обработки информации | | - | | - |  |  |  |  |
| ЗИС.15 | | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | | + | | + |  |  |  |  |
| ЗИС.16 | | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов | | - | | - |  |  |  |  |
| ЗИС.17 | | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | | + | | + |  |  |  |  |
| ЗИС.18 | | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения | | - | | - |  |  |  |  |
| ЗИС.19 | | Изоляция процессов (выполнение программ) в выделенной области памяти | | - | | - |  |  |  |  |
| ЗИС.20 | | Защита беспроводных соединений, применяемых в информационной системе | | + | | + |  |  |  |  |
| ЗИС.21 | | Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы | | - | | - |  |  |  |  |
| ЗИС.22 | | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании этой информационной системы | | - | | + |  |  |  |  |
| ЗИС.23 | | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 1) | | В информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности, общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 2) | | В информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия) | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 3) | | Оператор должен ограничить количество точек доступа в информационную систему из внешних информационных систем и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 4а) | | Оператором в информационной системе: должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 4б) | | Оператором в информационной системе: должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 4в) | | Оператором в информационной системе: 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 Российской Федерации | | - | | + |  |  |  |  |
| ЗИС.23  (усил. 5) | | В информационной системе должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено») | | - | | + |  |  |  |  |
| ЗИС.24 | | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | | - | | + |  |  |  |  |
| ЗИС.25 | | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) | | - | | - |  |  |  |  |
| ЗИС.26 | | Использование прикладного и специального программного обеспечения, имеющего возможность функционирования на различных типах операционных систем | | - | | - |  |  |  |  |
| ЗИС.27 | | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации | | - | | - |  |  |  |  |
| ЗИС.28 | | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание у нарушителя ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы | | - | | - |  |  |  |  |
| ЗИС.29 | | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновения отказов (сбоев) в системе защиты информации информационной системы | | - | | - |  |  |  |  |
| ЗИС.30 | | Защита мобильных технических средств, применяемых в информационной системе | | - | | + |  |  |  |  |
| 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 информационной системы и системы защиты персональных данных (УКФ) | | | | | | | | | | |
| УКФ.1 | | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | | + | | - |  |  |  |  |
| УКФ.2 | | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | | + | | - |  |  |  |  |
| УКФ.3 | | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | | + | | - |  |  |  |  |
| УКФ.4 | | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | | + | | - |  |  |  |  |
| XVI. Организационные меры по работе с СКЗИ (КЗИ) | | | | | | | | | | |
| КЗИ.1 | Обучение лиц, использующих СКЗИ, правилам работы с ними | |  | |  | |  |  |  |  |
| КЗИ.2 | Осуществление поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним | |  | |  | |  |  |  |  |
| КЗИ.3 | Определение лиц, допущенных к эксплуатации СКЗИ | |  | |  | |  |  |  |  |
| КЗИ.4 | Обеспечивается хранение ключевых носителей, эксплуатационной и технической документации к СКЗИ в шкафах (ящиках, хранилищах), исключающие бесконтрольный доступ к ним | |  | |  | |  |  |  |  |
| КЗИ.5 | СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы) | |  | |  | |  |  |  |  |
| КЗИ.6 | Ведение на каждого пользователя СКЗИ лицевого счета | |  | |  | |  |  |  |  |
| КЗИ.7 | Утверждение перечня лиц, имеющих право доступа в помещения, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ | |  | |  | |  |  |  |  |

1. Базовый набор мер в соответствии с Приказом ФСТЭК России № 21 с выборкой требований для 1 уровня защищенности персональных данных. [↑](#footnote-ref-1)
2. Базовый набор мер в соответствии с Приказом ФСТЭК России № 17 с выборкой требований для 2 класса защищенности персональных данных. [↑](#footnote-ref-2)
3. Адаптация базового набора мер защиты информации применительно к структурно-функциональным характеристикам ИС, информационным технологиям, особенностям функционирования ИС. [↑](#footnote-ref-3)
4. Уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации. [↑](#footnote-ref-4)
5. Дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных. [↑](#footnote-ref-5)
6. Обозначение «А» в графе «Итог» обозначает, что мера защиты информации актуальна для ИС. Обозначение «Н» в графе «Итог» обозначает, что мера неактуальная для ИС. [↑](#footnote-ref-6)