|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Условное обозначение и номер меры или документ** | **Приказ ФСТЭК России** | **Меры защиты информации в информационных системах** | **Базовый (К2, 1 КатЗн)[[1]](#footnote-1)** | **Адаптация  с учетом особенностей ИС[[2]](#footnote-2)** | **Уточнение с учетом модели угроз[[3]](#footnote-3)** | **Дополнение с учетом законодательства[[4]](#footnote-4)** | **Итог[[5]](#footnote-5)** |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | | | | | |
| ИАФ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур идентификации и аутентификации | + |  |  |  |
| ИАФ.1 | 17 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + |  |  |  | А |
| 239 | Идентификация и аутентификация пользователей и инициируемых ими процессов | + |  |  |  |
| ИАФ.2 | 17 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | + |  |  |  | А |
| 239 | Идентификация и аутентификация устройств | + |  |  |  |
| ИАФ.3 | 17 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + |  |  |  | А |
| 239 | Управление идентификаторами | + |  |  |  |
| ИАФ.4 | 17 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + |  |  |  | А |
| 239 | Управление средствами аутентификации | + |  |  |  |
| ИАФ.5 | 17 | Защита обратной связи при вводе аутентификационной информации | + |  |  |  | А |
| 239 | Идентификация и аутентификация внешних пользователей | + |  |  |  |
| ИАФ.6 | 17 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + |  |  |  | А (17) |
| 239 | Двусторонняя аутентификация | - |  |  |  |
| ИАФ.7 | 17 | 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 | - |  |  |  | А (239) |
| 239 | Защита аутентификационной информации при передаче | + |  |  |  |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | | | | | |
| УПД.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур управления доступом | + |  |  |  |
| УПД.1 | 17 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + |  |  |  | А |
| 239 | Управление учетными записями пользователей | + |  |  |  |
| УПД.2 | 17 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + |  |  |  | А |
| 239 | Реализация модели управления доступом | + |  |  |  |
| УПД.3 | 17 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + |  |  |  | А |
| 239 | Доверенная загрузка | + |  |  |  |
| УПД.4 | 17 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + |  |  |  | А |
| 239 | Разделение полномочий (ролей) пользователей | + |  |  |  |
| УПД.5 | 17 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + |  |  |  | А |
| 239 | Назначение минимально необходимых прав и привилегий | + |  |  |  |
| УПД.6 | 17 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + |  |  |  | А |
| 239 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему | + |  |  |  |
| УПД.7 | 17 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации | - |  |  |  | Н |
| 239 | Предупреждение пользователя при его доступе к информационным ресурсам | - |  |  |  |
| УПД.8 | 17 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему | - |  |  |  | Н |
| 239 | Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе | - |  |  |  |
| УПД.9 | 17 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы | - |  |  |  | А (239) |
| 239 | Ограничение числа параллельных сеансов доступа | + |  |  |  |
| УПД.10 | 17 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | + |  |  |  | А |
| 239 | Блокирование сеанса доступа пользователя при неактивности | + |  |  |  |
| УПД.11 | 17 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + |  |  |  | А |
| 239 | Управление действиями пользователей до идентификации и аутентификации | + |  |  |  |
| УПД.12 | 17 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки | - |  |  |  | Н |
| 239 | Управление атрибутами безопасности | - |  |  |  |
| УПД.13 | 17 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + |  |  |  | А |
| 239 | Реализация защищенного удаленного доступа | + |  |  |  |
| УПД.14 | 17 | Регламентация и контроль использования в информационной системе мобильных технических средств | + |  |  |  | А |
| 239 | Контроль доступа из внешних информационных (автоматизированных) систем | + |  |  |  |
| УПД.15 | 17 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + |  |  |  | А (17) |
| 239 | - | - | - | - | - |
| УПД.16 | 17 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + |  |  |  | А (17) |
| 239 | - | - | - | - | - |
| УПД.17 | 17 | Обеспечение доверенной загрузки средств вычислительной техники | + |  |  |  | А (17) |
| 239 | - | - | - | - | - |
| III. Ограничение программной среды (ОПС) | | | | | | | |
| ОПС.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур ограничения программной среды | + |  |  |  |
| ОПС.1 | 17 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения | - |  |  |  | А (239) |
| 239 | Управление запуском (обращениями) компонентов программного обеспечения | + |  |  |  |
| ОПС.2 | 17 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | + |  |  |  | А |
| 239 | Управление установкой (инсталляцией) компонентов программного обеспечения | + |  |  |  |
| ОПС.3 | 17 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | + |  |  |  | А (17) |
| 239 | Управление временными файлами | - |  |  |  |
| ОПС.4 | 17 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов | - |  |  |  | Н |
| 239 | - | - | - | - | - |
| IV. Защита машинных носителей информации (ЗНИ) | | | | | | | |
| ЗНИ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур защиты машинных носителей информации | + |  |  |  |
| ЗНИ.1 | 17 | Учет машинных носителей информации | + |  |  |  | А |
| 239 | Учет машинных носителей информации | + |  |  |  |
| ЗНИ.2 | 17 | Управление доступом к машинным носителям информации | + |  |  |  | А |
| 239 | Управление физическим доступом к машинным носителям информации | + |  |  |  |
| ЗНИ.3 | 17 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | - |  |  |  | Н |
| 239 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | - |  |  |  |
| ЗНИ.4 | 17 | Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах | - |  |  |  | Н |
| 239 | Исключение возможности несанкционированного чтения информации на машинных носителях информации | - |  |  |  |
| ЗНИ.5 | 17 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации | + |  |  |  | А |
| 239 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации | + |  |  |  |
| ЗНИ.6 | 17 | Контроль ввода (вывода) информации на машинные носители информации | - |  |  |  | А (239) |
| 239 | Контроль ввода (вывода) информации на съемные машинные носители информации | + |  |  |  |
| ЗНИ.7 | 17 | Контроль подключения машинных носителей информации | - |  |  |  | А (239) |
| 239 | Контроль подключения съемных машинных носителей информации | + |  |  |  |
| ЗНИ.8 | 17 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) | + |  |  |  | А |
| 239 | Уничтожение (стирание) информации на машинных носителях информации | + |  |  |  |
| V. Аудит безопасности (АУД) | | | | | | | |
| АУД.0 | 239 | Регламентация правил и процедур аудита безопасности | + |  |  |  | А (239) |
| АУД.1 | 239 | Инвентаризация информационных ресурсов | + |  |  |  | А (239) |
| АУД.2 | 239 | Анализ уязвимостей и их устранение | + |  |  |  | А (239) |
| АУД.3 | 239 | Генерирование временных меток и (или) синхронизация системного времени | + |  |  |  | А (239) |
| АУД.4 | 239 | Регистрация событий безопасности | + |  |  |  | А (239) |
| АУД.5 | 239 | Контроль и анализ сетевого трафика | - |  |  |  | Н |
| АУД.6 | 239 | Защита информации о событиях безопасности | + |  |  |  | А (239) |
| АУД.7 | 239 | Мониторинг безопасности | + |  |  |  | А (239) |
| АУД.8 | 239 | Реагирование на сбои при регистрации событий безопасности | + |  |  |  | А (239) |
| АУД.9 | 239 | Анализ действий отдельных пользователей | + |  |  |  | А (239) |
| АУД.10 | 239 | Проведение внутренних аудитов | + |  |  |  | А (239) |
| АУД.11 | 239 | Проведение внешних аудитов | - |  |  |  | Н |
| VI. Регистрация событий безопасности (РСБ) | | | | | | | |
| РСБ.1 | 17 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + |  |  |  | А (17) |
| РСБ.2 | 17 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + |  |  |  | А (17) |
| РСБ.3 | 17 | Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения | + |  |  |  | А (17) |
| РСБ.4 | 17 | 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 | + |  |  |  | А (17) |
| РСБ.5 | 17 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + |  |  |  | А (17) |
| РСБ.6 | 17 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | + |  |  |  | А (17) |
| РСБ.7 | 17 | Защита информации о событиях безопасности | + |  |  |  | А (17) |
| РСБ.8 | 17 | Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе | - |  |  |  | Н |
| VII. Антивирусная защита (АВЗ) | | | | | | | |
| АВЗ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур антивирусной защиты | + |  |  |  |
| АВЗ.1 | 17 | Реализация антивирусной защиты | + |  |  |  | А |
| 239 | Реализация антивирусной защиты | + |  |  |  |
| АВЗ.2 | 17 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + |  |  |  | А |
| 239 | Антивирусная защита электронной почты и иных сервисов | + |  |  |  |
| АВЗ.3 | 17 | - | - | - | - | - | А (239) |
| 239 | Контроль использования архивных, исполняемых и зашифрованных файлов | + |  |  |  |
| АВЗ.4 | 17 | - | - | - | - | - | А (239) |
| 239 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + |  |  |  |
| АВЗ.5 | 17 | - | - | - | - | - | А (239) |
| 239 | Использование средств антивирусной защиты различных производителей | + |  |  |  |
| VIII. Обнаружение вторжений (СОВ)  Предотвращение вторжений (компьютерных атак) (СОВ) | | | | | | | |
| СОВ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур предотвращения вторжений (компьютерных атак) | + |  |  |  |
| СОВ.1 | 17 | Обнаружение вторжений | + |  |  |  | А |
| 239 | Обнаружение и предотвращение компьютерных атак | + |  |  |  |
| СОВ.2 | 17 | Обновление базы решающих правил | + |  |  |  | А |
| 239 | Обновление базы решающих правил | + |  |  |  |
| IX. Контроль (анализ) защищенности информации (АНЗ) | | | | | | | |
| АНЗ.1 | 17 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | + |  |  |  | А (17) |
| АНЗ.2 | 17 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + |  |  |  | А (17) |
| АНЗ.3 | 17 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | + |  |  |  | А (17) |
| АНЗ.4 | 17 | Контроль состава технических средств, программного обеспечения и средств защиты информации | + |  |  |  | А (17) |
| АНЗ.5 | 17 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе | + |  |  |  | А (17) |
| X. Обеспечение целостности информационной системы и информации (ОЦЛ) | | | | | | | |
| ОЦЛ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур обеспечения целостности | + |  |  |  |
| ОЦЛ.1 | 17 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | + |  |  |  | А |
| 239 | Контроль целостности программного обеспечения | + |  |  |  |
| ОЦЛ.2 | 17 | Контроль целостности информации, содержащейся в базах данных информационной системы | - |  |  |  | Н |
| 239 | Контроль целостности информации | - |  |  |  |
| ОЦЛ.3 | 17 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | + |  |  |  | А |
| 239 | Ограничения по вводу информации в информационную (автоматизированную) систему | + |  |  |  |
| ОЦЛ.4 | 17 | 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) | + |  |  |  | А |
| 239 | Контроль данных, вводимых в информационную (автоматизированную) систему | + |  |  |  |
| ОЦЛ.5 | 17 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы | - |  |  |  | А (239) |
| 239 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | + |  |  |  |
| ОЦЛ.6 | 17 | Ограничение прав пользователей по вводу информации в информационную систему | - |  |  |  | Н |
| 239 | Обезличивание и (или) деидентификация информации | - |  |  |  |
| ОЦЛ.7 | 17 | Контроль точности, полноты и правильности данных, вводимых в информационную систему | - |  |  |  | Н |
| 239 | - | - | - | - | - |
| ОЦЛ.8 | 17 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | - |  |  |  | Н |
| 239 | - | - | - | - | - |
| XI. Обеспечение доступности информации (ОДТ) | | | | | | | |
| ОДТ.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур обеспечения доступности | + |  |  |  |
| ОДТ.1 | 17 | Использование отказоустойчивых технических средств | - |  |  |  | А (239) |
| 239 | Использование отказоустойчивых технических средств | + |  |  |  |
| ОДТ.2 | 17 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | - |  |  |  | А (239) |
| 239 | Резервирование средств и систем | + |  |  |  |
| ОДТ.3 | 17 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | + |  |  |  | А |
| 239 | Контроль безотказного функционирования средств и систем | + |  |  |  |
| ОДТ.4 | 17 | Периодическое резервное копирование информации на резервные машинные носители информации | + |  |  |  | А |
| 239 | Резервное копирование информации | + |  |  |  |
| ОДТ.5 | 17 | Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала | + |  |  |  | А |
| 239 | Обеспечение возможности восстановления информации | + |  |  |  |
| ОДТ.6 | 17 | Кластеризация информационной системы и (или) ее сегментов | - |  |  |  | А (239) |
| 239 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях | + |  |  |  |
| ОДТ.7 | 17 | Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации | + |  |  |  | А (17) |
| 239 | Кластеризация информационной (автоматизированной) системы | - |  |  |  |
| ОДТ.8 | 17 | - | - | - | - | - | А (239) |
| 239 | Контроль предоставляемых вычислительных ресурсов и каналов связи | + |  |  |  |
| XII. Защита технических средств и систем (ЗТС) | | | | | | | |
| ЗТС.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур защиты технических средств и систем | + |  |  |  |
| ЗТС.1 | 17 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | - |  |  |  | Н |
| 239 | Защита информации от утечки по техническим каналам | - |  |  |  |
| ЗТС.2 | 17 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | + |  |  |  | А |
| 239 | Организация контролируемой зоны | + |  |  |  |
| ЗТС.3 | 17 | 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 | + |  |  |  | А |
| 239 | Управление физическим доступом | + |  |  |  |
| ЗТС.4 | 17 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |  |  |  | А |
| 239 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |  |  |  |
| ЗТС.5 | 17 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | - |  |  |  | А (239) |
| 239 | Защита от внешних воздействий | + |  |  |  |
| ЗТС.6 | 17 | - | - | - | - | - | Н |
| 239 | Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации | - |  |  |  |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | | | | | |
| ЗИС.0 | 17 | - | - | - | - | - | А (239) |
| 239 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов | + |  |  |  |
| ЗИС.1 | 17 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы | + |  |  |  | А |
| 239 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями | + |  |  |  |
| ЗИС.2 | 17 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | - |  |  |  | А (239) |
| 239 | Защита периметра информационной (автоматизированной) системы | + |  |  |  |
| ЗИС.3 | 17 | 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 | + |  |  |  | А |
| 239 | Эшелонированная защита информационной (автоматизированной) системы | + |  |  |  |
| ЗИС.4 | 17 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | - |  |  |  | А (239) |
| 239 | Сегментирование информационной (автоматизированной) системы | + |  |  |  |
| ЗИС.5 | 17 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | + |  |  |  | А |
| 239 | Организация демилитаризованной зоны | + |  |  |  |
| ЗИС.6 | 17 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами | - |  |  |  | А (239) |
| 239 | Управление сетевыми потоками | + |  |  |  |
| ЗИС.7 | 17 | 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 | + |  |  |  | А (17) |
| 239 | Использование эмулятора среды функционирования программного обеспечения ("песочница") | - |  |  |  |
| ЗИС.8 | 17 | 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 | + |  |  |  | А |
| 239 | Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы | + |  |  |  |
| ЗИС.9 | 17 | 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 | + |  |  |  | А (17) |
| 239 | Создание гетерогенной среды | - |  |  |  |
| ЗИС.10 | 17 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | - |  |  |  | Н |
| 239 | Использование программного обеспечения, функционирующего в средах различных операционных систем | - | - | - | - |
| ЗИС.11 | 17 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | + |  |  |  | А (17) |
| 239 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | - |  |  |  |
| ЗИС.12 | 17 | Исключение возможности отрицания пользователем факта отправки информации другому пользователю | + |  |  |  | А (17) |
| 239 | Изоляция процессов (выполнение программ) в выделенной области памяти | - |  |  |  |
| ЗИС.13 | 17 | Исключение возможности отрицания пользователем факта получения информации от другого пользователя | + |  |  |  | А |
| 239 | Защита неизменяемых данных | + |  |  |  |
| ЗИС.14 | 17 | Использование устройств терминального доступа для обработки информации | - |  |  |  | Н |
| 239 | Использование неперезаписываемых машинных носителей информации | - |  |  |  |
| ЗИС.15 | 17 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации | + |  |  |  | А (17) |
| 239 | Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек | - |  |  |  |
| ЗИС.16 | 17 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов | - |  |  |  | А (239) |
| 239 | Защита от спама | + |  |  |  |
| ЗИС.17 | 17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | + |  |  |  | А (17) |
| 239 | Защита информации от утечек | - |  |  |  |
| ЗИС.18 | 17 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения | - |  |  |  | Н |
| 239 | Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию | - |  |  |  |
| ЗИС.19 | 17 | Изоляция процессов (выполнение программ) в выделенной области памяти | - |  |  |  | А (239) |
| 239 | Защита информации при ее передаче по каналам связи | + |  |  |  |
| ЗИС.20 | 17 | Защита беспроводных соединений, применяемых в информационной системе | + |  |  |  | А |
| 239 | Обеспечение доверенных канала, маршрута | + |  |  |  |
| ЗИС.21 | 17 | 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 | - |  |  |  | А (239) |
| 239 | Запрет несанкционированной удаленной активации периферийных устройств | + |  |  |  |
| ЗИС.22 | 17 | Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы | + |  |  |  | А (17) |
| 239 | Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами | - |  |  |  |
| ЗИС.23 | 17 | Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями | + |  |  |  | А (17) |
| 239 | Контроль использования мобильного кода | - |  |  |  |
| ЗИС.24 | 17 | Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения | + |  |  |  | А (17) |
| 239 | Контроль передачи речевой информации | - |  |  |  |
| ЗИС.25 | 17 | Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды) | - |  |  |  | Н |
| 239 | Контроль передачи видеоинформации | - |  |  |  |
| ЗИС.26 | 17 | Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем | - |  |  |  | Н |
| 239 | Подтверждение происхождения источника информации | - |  |  |  |
| ЗИС.27 | 17 | Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации | - |  |  |  | А (239) |
| 239 | Обеспечение подлинности сетевых соединений | + |  |  |  |
| ЗИС.28 | 17 | Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы | - |  |  |  | Н |
| 239 | Исключение возможности отрицания отправки информации | - |  |  |  |
| ЗИС.29 | 17 | Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы | - |  |  |  | Н |
| 239 | Исключение возможности отрицания получения информации | - |  |  |  |
| ЗИС.30 | 17 | Защита мобильных технических средств, применяемых в информационной системе | + |  |  |  | А (17) |
| 239 | Использование устройств терминального доступа | - |  |  |  |
| ЗИС.31 | 17 | - | - | - | - | - | Н |
| 239 | Защита от скрытых каналов передачи информации | - |  |  |  |
| ЗИС.32 | 17 | - | - | - | - | - | А (239) |
| 239 | Защита беспроводных соединений | + |  |  |  |
| ЗИС.33 | 17 | - | - | - | - | - | А (239) |
| 239 | Исключение доступа через общие ресурсы | + |  |  |  |
| ЗИС.34 | 17 | - | - | - | - | - | А (239) |
| 239 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) | + |  |  |  |
| ЗИС.35 | 17 | - | - | - | - | - | А (239) |
| 239 | Управление сетевыми соединениями | + |  |  |  |
| ЗИС.36 | 17 | - | - | - | - | - | Н |
| 239 | Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем | - |  |  |  |
| ЗИС.37 | 17 | - | - | - | - | - | Н |
| 239 | Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев) | - |  |  |  |
| ЗИС.38 | 17 | - | - | - | - | - | А (239) |
| 239 | Защита информации при использовании мобильных устройств | + |  |  |  |
| ЗИС.39 | 17 | - | - | - | - | - | А (239) |
| 239 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + |  |  |  |
| XIV. Защита среды виртуализации (ЗСВ) | | | | | | | |
| ЗСВ.1 | 17 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + |  |  |  | А (17) |
| ЗСВ.2 | 17 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + |  |  |  | А (17) |
| ЗСВ.3 | 17 | Регистрация событий безопасности в виртуальной инфраструктуре | + |  |  |  | А (17) |
| ЗСВ.4 | 17 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | + |  |  |  | А (17) |
| ЗСВ.5 | 17 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией | - |  |  |  | Н |
| ЗСВ.6 | 17 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + |  |  |  | А (17) |
| ЗСВ.7 | 17 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | + |  |  |  | А (17) |
| ЗСВ.8 | 17 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | + |  |  |  | А (17) |
| ЗСВ.9 | 17 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | + |  |  |  | А (17) |
| ЗСВ.10 | 17 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей | + |  |  |  | А (17) |
| XV. Реагирование на компьютерные инциденты (ИНЦ) | | | | | | | |
| ИНЦ.0 | 239 | Регламентация правил и процедур реагирования на компьютерные инциденты | + |  |  |  | А (239) |
| ИНЦ.1 | 239 | Выявление компьютерных инцидентов | + |  |  |  | А (239) |
| ИНЦ.2 | 239 | Информирование о компьютерных инцидентах | + |  |  |  | А (239) |
| ИНЦ.3 | 239 | Анализ компьютерных инцидентов | + |  |  |  | А (239) |
| ИНЦ.4 | 239 | Устранение последствий компьютерных инцидентов | + |  |  |  | А (239) |
| ИНЦ.5 | 239 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов | + |  |  |  | А (239) |
| ИНЦ.6 | 239 | Хранение и защита информации о компьютерных инцидентах | + |  |  |  | А (239) |
| XVI. Управление конфигурацией (УКФ) | | | | | | | |
| УКФ.0 | 239 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы | + |  |  |  | А (239) |
| УКФ.1 | 239 | Идентификация объектов управления конфигурацией | - |  |  |  | Н |
| УКФ.2 | 239 | Управление изменениями | + |  |  |  | А (239) |
| УКФ.3 | 239 | Установка (инсталляция) только разрешенного к использованию программного обеспечения | + |  |  |  | А (239) |
| УКФ.4 | 239 | Контроль действий по внесению изменений | - |  |  |  | Н |
| XVII. Управление обновлениями программного обеспечения (ОПО) | | | | | | | |
| ОПО.0 | 239 | Регламентация правил и процедур управления обновлениями программного обеспечения | + |  |  |  | А (239) |
| ОПО.1 | 239 | Поиск, получение обновлений программного обеспечения от доверенного источника | + |  |  |  | А (239) |
| ОПО.2 | 239 | Контроль целостности обновлений программного обеспечения | + |  |  |  | А (239) |
| ОПО.3 | 239 | Тестирование обновлений программного обеспечения | + |  |  |  | А (239) |
| ОПО.4 | 239 | Установка обновлений программного обеспечения | + |  |  |  | А (239) |
| XVIII. Планирование мероприятий по обеспечению безопасности (ПЛН) | | | | | | | |
| ПЛН.0 | 239 | Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации | + |  |  |  | А (239) |
| ПЛН.1 | 239 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | + |  |  |  | А (239) |
| ПЛН.2 | 239 | Контроль выполнения мероприятий по обеспечению защиты информации | + |  |  |  | А (239) |
| XIX. Обеспечение действий в нештатных ситуациях (ДНС) | | | | | | | |
| ДНС.0 | 239 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | + |  |  |  | А (239) |
| ДНС.1 | 239 | Разработка плана действий в нештатных ситуациях | + |  |  |  | А (239) |
| ДНС.2 | 239 | Обучение и отработка действий персонала в нештатных ситуациях | + |  |  |  | А (239) |
| ДНС.3 | 239 | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций | + |  |  |  | А (239) |
| ДНС.4 | 239 | Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций | + |  |  |  | А (239) |
| ДНС.5 | 239 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций | + |  |  |  | А (239) |
| ДНС.6 | 239 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения | + |  |  |  | А (239) |
| XX. Информирование и обучение персонала (ИПО) | | | | | | | |
| ИПО.0 | 239 | Регламентация правил и процедур информирования и обучения персонала | + |  |  |  | А (239) |
| ИПО.1 | 239 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | + |  |  |  | А (239) |
| ИПО.2 | 239 | Обучение персонала правилам безопасной работы | + |  |  |  | А (239) |
| ИПО.3 | 239 | Проведение практических занятий с персоналом по правилам безопасной работы | + |  |  |  | А (239) |
| ИПО.4 | 239 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы | + |  |  |  | А (239) |
| XXI. Организационные меры по работе с СКЗИ (КЗИ) | | | | | | | |
| КЗИ.1 | 524 (ФСБ) | Обучение лиц, использующих СКЗИ, правилам работы с ними |  |  |  |  |  |
| КЗИ.2 | 524 (ФСБ) | Осуществление поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним |  |  |  |  |  |
| КЗИ.3 | 524 (ФСБ) | Определение лиц, допущенных к эксплуатации СКЗИ |  |  |  |  |  |
| КЗИ.4 | 524 (ФСБ) | Обеспечивается хранение ключевых носителей, эксплуатационной и технической документации к СКЗИ в шкафах (ящиках, хранилищах), исключающие бесконтрольный доступ к ним |  |  |  |  |  |
| КЗИ.5 | 524 (ФСБ) | СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы) |  |  |  |  |  |
| КЗИ.6 | 524 (ФСБ) | Ведение на каждого пользователя СКЗИ лицевого счета |  |  |  |  |  |
| КЗИ.7 | 524 (ФСБ) | 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 № 17 с выборкой требований для 2 класса защищенности и Приказом ФСТЭК России №239 с выборкой требований по 1 категории значимости. [↑](#footnote-ref-1)
2. Адаптация базового набора мер защиты информации применительно к структурно-функциональным характеристикам ИС, информационным технологиям, особенностям функционирования ИС. [↑](#footnote-ref-2)
3. 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-3)
4. 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 информации. [↑](#footnote-ref-4)
5. 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-5)