| **Условное обозначение и номер меры или документ** | **Меры** **обеспечения безопасности значимого объекта** | **Приказ № 239 ФСТЭК России[[1]](#footnote-1)**  **(1 категория)** | **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 (ИАФ) | | | | | | |
| ИАФ.0 | Регламентация правил и процедур идентификации и аутентификации | + |  |  |  |  |
| ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов | + |  |  |  |  |
| ИАФ.2 | Идентификация и аутентификация устройств | + |  |  |  |  |
| ИАФ.3 | Управление идентификаторами | + |  |  |  |  |
| ИАФ.4 | Управление средствами аутентификации | + |  |  |  |  |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей | + |  |  |  |  |
| ИАФ.6 | Двусторонняя аутентификация | - |  |  |  |  |
| ИАФ.7 | Защита аутентификационной информации при передаче | + |  |  |  |  |
| II. Управление доступом (УПД) | | | | | | |
| УПД.0 | Регламентация правил и процедур управления доступом | + |  |  |  |  |
| УПД.1 | Управление учетными записями пользователей | + |  |  |  |  |
| УПД.2 | Реализация модели управления доступом | + |  |  |  |  |
| УПД.3 | Доверенная загрузка | + |  |  |  |  |
| УПД.4 | Разделение полномочий (ролей) пользователей | + |  |  |  |  |
| УПД.5 | Назначение минимально необходимых прав и привилегий | + |  |  |  |  |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему | + |  |  |  |  |
| УПД.7 | Предупреждение пользователя при его доступе к информационным ресурсам | - |  |  |  |  |
| УПД.8 | Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе | - |  |  |  |  |
| УПД.9 | Ограничение числа параллельных сеансов доступа | + |  |  |  |  |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности | + |  |  |  |  |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации | + |  |  |  |  |
| УПД.12 | Управление атрибутами безопасности | - |  |  |  |  |
| УПД.13 | Реализация защищенного удаленного доступа | + |  |  |  |  |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем | + |  |  |  |  |
| III. Ограничение программной среды (ОПС) | | | | | | |
| ОПС.0 | Регламентация правил и процедур ограничения программной среды | + |  |  |  |  |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения | + |  |  |  |  |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения | + |  |  |  |  |
| ОПС.3 | Управление временными файлами | - |  |  |  |  |
| IV. Защита машинных носителей информации (ЗНИ) | | | | | | |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации | + |  |  |  |  |
| ЗНИ.1 | Учет машинных носителей информации | + |  |  |  |  |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации | + |  |  |  |  |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | - |  |  |  |  |
| ЗНИ.4 | Исключение возможности несанкционированного чтения информации на машинных носителях информации | - |  |  |  |  |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации | + |  |  |  |  |
| ЗНИ.6 | Контроль ввода (вывода) информации на съемные машинные носители информации | + |  |  |  |  |
| ЗНИ.7 | Контроль подключения съемных машинных носителей информации | + |  |  |  |  |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях информации | + |  |  |  |  |
| V. Аудит безопасности (АУД) | | | | | | |
| АУД.0 | Регламентация правил и процедур аудита безопасности | + |  |  |  |  |
| АУД.1 | Инвентаризация информационных ресурсов | + |  |  |  |  |
| АУД.2 | Анализ уязвимостей и их устранение | + |  |  |  |  |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | + |  |  |  |  |
| АУД.4 | Регистрация событий безопасности | + |  |  |  |  |
| АУД.5 | Контроль и анализ сетевого трафика | + |  |  |  |  |
| АУД.6 | Защита информации о событиях безопасности | + |  |  |  |  |
| АУД.7 | Мониторинг безопасности | + |  |  |  |  |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности | + |  |  |  |  |
| АУД.9 | Анализ действий отдельных пользователей | + |  |  |  |  |
| АУД.10 | Проведение внутренних аудитов | + |  |  |  |  |
| АУД.11 | Проведение внешних аудитов | - |  |  |  |  |
| VI. Антивирусная защита (АВЗ) | | | | | | |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты | + |  |  |  |  |
| АВЗ.1 | Реализация антивирусной защиты | + |  |  |  |  |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов | + |  |  |  |  |
| АВЗ.3 | Контроль использования архивных, исполняемых и зашифрованных файлов | + |  |  |  |  |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + |  |  |  |  |
| АВЗ.5 | Использование средств антивирусной защиты различных производителей | + |  |  |  |  |
| VII. Предотвращение вторжений (компьютерных атак) (СОВ) | | | | | | |
| СОВ.0 | Регламентация правил и процедур предотвращения вторжений (компьютерных атак) | + |  |  |  |  |
| СОВ.1 | Обнаружение и предотвращение компьютерных атак | + |  |  |  |  |
| СОВ.2 | Обновление базы решающих правил | + |  |  |  |  |
| VIII. Обеспечение целостности (ОЦЛ) | | | | | | |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности | + |  |  |  |  |
| ОЦЛ.1 | Контроль целостности программного обеспечения | + |  |  |  |  |
| ОЦЛ.2 | Контроль целостности информации | - |  |  |  |  |
| ОЦЛ.3 | Ограничения по вводу информации в информационную (автоматизированную) систему | + |  |  |  |  |
| ОЦЛ.4 | Контроль данных, вводимых в информационную (автоматизированную) систему | + |  |  |  |  |
| ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | + |  |  |  |  |
| ОЦЛ.6 | Обезличивание и (или) деидентификация информации | - |  |  |  |  |
| IX. Обеспечение доступности (ОДТ) | | | | | | |
| ОДТ.0 | Регламентация правил и процедур обеспечения доступности | + |  |  |  |  |
| ОДТ.1 | Использование отказоустойчивых технических средств | + |  |  |  |  |
| ОДТ.2 | Резервирование средств и систем | + |  |  |  |  |
| ОДТ.3 | Контроль безотказного функционирования средств и систем | + |  |  |  |  |
| ОДТ.4 | Резервное копирование информации | + |  |  |  |  |
| ОДТ.5 | Обеспечение возможности восстановления информации | + |  |  |  |  |
| ОДТ.6 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях | + |  |  |  |  |
| ОДТ.7 | Кластеризация информационной (автоматизированной) системы | - |  |  |  |  |
| ОДТ.8 | Контроль предоставляемых вычислительных ресурсов и каналов связи | + |  |  |  |  |
| X. Защита технических средств и систем (ЗТС) | | | | | | |
| ЗТС.0 | Регламентация правил и процедур защиты технических средств и систем | + |  |  |  |  |
| ЗТС.1 | Защита информации от утечки по техническим каналам | - |  |  |  |  |
| ЗТС.2 | Организация контролируемой зоны | + |  |  |  |  |
| ЗТС.3 | Управление физическим доступом | + |  |  |  |  |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |  |  |  |  |
| ЗТС.5 | Защита от внешних воздействий | + |  |  |  |  |
| ЗТС.6 | Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации | - |  |  |  |  |
| XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) | | | | | | |
| ЗИС.0 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов | + |  |  |  |  |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями | + |  |  |  |  |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы | + |  |  |  |  |
| ЗИС.3 | Эшелонированная защита информационной (автоматизированной) системы | + |  |  |  |  |
| ЗИС.4 | Сегментирование информационной (автоматизированной) системы | + |  |  |  |  |
| ЗИС.5 | Организация демилитаризованной зоны | + |  |  |  |  |
| ЗИС.6 | Управление сетевыми потоками | + |  |  |  |  |
| ЗИС.7 | Использование эмулятора среды функционирования программного обеспечения ("песочница") | - |  |  |  |  |
| ЗИС.8 | Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы | + |  |  |  |  |
| ЗИС.9 | Создание гетерогенной среды | - |  |  |  |  |
| ЗИС.10 | Использование программного обеспечения, функционирующего в средах различных операционных систем | - |  |  |  |  |
| ЗИС.11 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | - |  |  |  |  |
| ЗИС.12 | Изоляция процессов (выполнение программ) в выделенной области памяти | - |  |  |  |  |
| ЗИС.13 | Защита неизменяемых данных | + |  |  |  |  |
| ЗИС.14 | Использование неперезаписываемых машинных носителей информации | - |  |  |  |  |
| ЗИС.15 | Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек | - |  |  |  |  |
| ЗИС.16 | Защита от спама | + |  |  |  |  |
| ЗИС.17 | Защита информации от утечек | - |  |  |  |  |
| ЗИС.18 | Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию | - |  |  |  |  |
| ЗИС.19 | Защита информации при ее передаче по каналам связи | + |  |  |  |  |
| ЗИС.20 | Обеспечение доверенных канала, маршрута | + |  |  |  |  |
| ЗИС.21 | Запрет несанкционированной удаленной активации периферийных устройств | + |  |  |  |  |
| ЗИС.22 | Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами | - |  |  |  |  |
| ЗИС.23 | Контроль использования мобильного кода | - |  |  |  |  |
| ЗИС.24 | Контроль передачи речевой информации | - |  |  |  |  |
| ЗИС.25 | Контроль передачи видеоинформации | - |  |  |  |  |
| ЗИС.26 | Подтверждение происхождения источника информации | - |  |  |  |  |
| ЗИС.27 | Обеспечение подлинности сетевых соединений | + |  |  |  |  |
| ЗИС.28 | Исключение возможности отрицания отправки информации | - |  |  |  |  |
| ЗИС.29 | Исключение возможности отрицания получения информации | - |  |  |  |  |
| ЗИС.30 | Использование устройств терминального доступа | - |  |  |  |  |
| ЗИС.31 | Защита от скрытых каналов передачи информации | - |  |  |  |  |
| ЗИС.32 | Защита беспроводных соединений | + |  |  |  |  |
| ЗИС.33 | Исключение доступа через общие ресурсы | + |  |  |  |  |
| ЗИС.34 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) | + |  |  |  |  |
| ЗИС.35 | Управление сетевыми соединениями | + |  |  |  |  |
| ЗИС.36 | Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем | - |  |  |  |  |
| ЗИС.37 | Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев) | - |  |  |  |  |
| ЗИС.38 | Защита информации при использовании мобильных устройств | + |  |  |  |  |
| ЗИС.39 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | + |  |  |  |  |
| XII. Реагирование на компьютерные инциденты (ИНЦ) | | | | | | |
| ИНЦ.0 | Регламентация правил и процедур реагирования на компьютерные инциденты | + |  |  |  |  |
| ИНЦ.1 | Выявление компьютерных инцидентов | + |  |  |  |  |
| ИНЦ.2 | Информирование о компьютерных инцидентах | + |  |  |  |  |
| ИНЦ.3 | Анализ компьютерных инцидентов | + |  |  |  |  |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов | + |  |  |  |  |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов | + |  |  |  |  |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах | + |  |  |  |  |
| XIII. Управление конфигурацией (УКФ) | | | | | | |
| УКФ.0 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы | + |  |  |  |  |
| УКФ.1 | Идентификация объектов управления конфигурацией | - |  |  |  |  |
| УКФ.2 | Управление изменениями | + |  |  |  |  |
| УКФ.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения | + |  |  |  |  |
| УКФ.4 | Контроль действий по внесению изменений | - |  |  |  |  |
| XIV. Управление обновлениями программного обеспечения (ОПО) | | | | | | |
| ОПО.0 | Регламентация правил и процедур управления обновлениями программного обеспечения | + |  |  |  |  |
| ОПО.1 | Поиск, получение обновлений программного обеспечения от доверенного источника | + |  |  |  |  |
| ОПО.2 | Контроль целостности обновлений программного обеспечения | + |  |  |  |  |
| ОПО.3 | Тестирование обновлений программного обеспечения | + |  |  |  |  |
| ОПО.4 | Установка обновлений программного обеспечения | + |  |  |  |  |
| XV. Планирование мероприятий по обеспечению безопасности (ПЛН) | | | | | | |
| ПЛН.0 | Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации | + |  |  |  |  |
| ПЛН.1 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | + |  |  |  |  |
| ПЛН.2 | Контроль выполнения мероприятий по обеспечению защиты информации | + |  |  |  |  |
| XVI. Обеспечение действий в нештатных ситуациях (ДНС) | | | | | | |
| ДНС.0 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | + |  |  |  |  |
| ДНС.1 | Разработка плана действий в нештатных ситуациях | + |  |  |  |  |
| ДНС.2 | Обучение и отработка действий персонала в нештатных ситуациях | + |  |  |  |  |
| ДНС.3 | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций | + |  |  |  |  |
| ДНС.4 | Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций | + |  |  |  |  |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций | + |  |  |  |  |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения | + |  |  |  |  |
| XVII. Информирование и обучение персонала (ИПО) | | | | | | |
| ИПО.0 | Регламентация правил и процедур информирования и обучения персонала | + |  |  |  |  |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | + |  |  |  |  |
| ИПО.2 | Обучение персонала правилам безопасной работы | + |  |  |  |  |
| ИПО.3 | Проведение практических занятий с персоналом по правилам безопасной работы | + |  |  |  |  |
| ИПО.4 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы | + |  |  |  |  |
| XVIII. 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 № 239 с выборкой требований для 1 категории значимости объекта критической информационной инфраструктуры. [↑](#footnote-ref-1)
2. Адаптация базового набора мер обеспечения безопасности значимого объекта применительно к структурно-функциональным характеристикам объекта критической информационной инфраструктуры, информационным технологиям, особенностям функционирования объекта критической информационной инфраструктуры. [↑](#footnote-ref-2)
3. Уточнение адаптированного базового набора мер обеспечения безопасности значимого объекта критической информационной инфраструктуры с учетом не выбранных ранее мер обеспечения безопасности значимого объекта критической информационной инфраструктуры для блокирования (нейтрализации) всех угроз безопасности объекта критической информационной инфраструктуры, включенных в модель угроз безопасности информации. [↑](#footnote-ref-3)
4. Дополнение уточненного адаптированного базового набора мер обеспечения безопасности значимого объекта критической информационной инфраструктуры мерами, обеспечивающими выполнение требований об обеспечении безопасности значимого объекта критической информационной инфраструктуры, установленными иными нормативными правовыми актами в области обеспечения безопасности значимого объекта критической информационной инфраструктуры. [↑](#footnote-ref-4)
5. Обозначение «А» в графе «Итог» обозначает, что мера обеспечения безопасности значимого объекта критической информационной инфраструктуры актуальна для ИС. Обозначение «Н» в графе «Итог» обозначает, что мера неактуальная для объекта критической информационной инфраструктуры. [↑](#footnote-ref-5)