Требования Приказа ФСТЭК №117, выполнение которых обеспечивает межсетевой экран ИКС ФСТЭК

В Приказе ФСТЭК №117 установлены меры защиты информации, включая организационные и технические. Указанные меры реализуются с помощью разных решений для информационной безопасности. В таблице представлен полный перечень требований и отмечены, выполнение каких из них **обеспечивает межсетевой экран ИКС**, сертифицированный ФСТЭК (сертификат №4832 от 02.08.2024 г.).

№ п.	Требования	Механизм реализации в ИКС ФСТЭК
п. 63а	Идентификация и аутентификация	Авторизация по IP- и MAC-адресу. Авторизация Captive Portal. Возможность синхронизации и авторизации пользователей через LDAP. Поддержка Active Directory, FreeIPA (ALD Pro), Samba DC.
п. 63б	Управление доступом	Межсетевой экран (Firewall) — фильтрация трафика на основе IP-адресов, портов, протоколов, MAC-адресов. Контроль приложений (Application Firewall) — разрешение/блокировка доступа к конкретным приложениям и сервисам.
п. 63в п. 49	Регистрация событий безопасности	IDS/IPS — ведение журналирования инцидентов информационной безопасности. Система логирования — регистрация попыток доступа, подключения пользователей, изменения правил, административные действия. Формирование отчетов по требованиям. Соединение с SIEM по протоколу syslog.
п. 63м п. 47	Защита точек беспроводного доступа	Межсетевой экран (Firewall) — изоляция Wi-Fi-сегмента от корпоративной сети.
п. 63о	Обнаружение и предотвращение вторжений на сетевом уровне	IDS/IPS — блокирует попытки несанкционированного доступа, эксплойты, ботнеты, DoS-атаки, вирусную активность в сети, spyware, TOR, анонимайзеры, телеметрию Windows и скомпрометированные IP-адреса.
п. 63п	Сегментация и межсетевое экранирование	Межсетевой экран — защищает сеть организации от различных внешних угроз; контролирует движение трафика на уровне IP-

		адресов и портов; позволяет настроить запрещающие и разрешающие правила, указать приоритеты.
п. 63р	Защита от компьютерных атак, направленных на отказ в обслуживании	IDS/IPS — защита от DoS-атак. МЭ — ограничивает количество подключений к ИКС. Fail2ban — защищает от брутфорс-атак (защита от перебора паролей и многократного подключения).
п. 40 п. 59	Контентная фильтрация и контроль доступа в интернет	Контент-фильтр ИКС — отвечает за блокировку нежелательной информации по словам и выражениям. Обновление списков Минюста и максимально быстрое реагирование на возникающие угрозы. МЭ — контроль трафика, возможность блокировки по геолокации.
п. 55	Резервное копирование	Ручное и автоматическое резервное копирование настроек системы, файлов статистики, баз данных веб-ресурсов и содержимого файлового сервера.
п. 55	Кластеризация	Кластер отказоустойчивости (работает в режиме active/standby).
п. 55	Агрегация каналов	Позволяет объединить несколько физических каналов в один логический в режимах: failover, lacp, loadbalance и broadcast. Такое объединение позволяет увеличивать пропускную способность и надежность канала.
п. 72	Класс защиты средств защиты информации (для ГИС 1 класса)	Сертификат ФСТЭК №4832 — МЭ типа «А» и «Б» 4 класса, СОВ 4 класса (соответствует требованиям для 1 класса защищенности).
Другие требования п. 63		
п. 63г	Защита виртуализации и облачных вычислений	-
п. 63д	Защита технологий контейнерных сред и их оркестрации	-
п. 63е	Защита сервисов электронной почты	-

п. 63ж	Защита веб-технологий	-
п. 63з	Защита программных интерфейсов взаимодействия приложений	-
п. 63и	Защита конечных устройств	-
п. 63к	Защита мобильных устройств	-
п. 63л	Защита технологий интернета вещей	-
п. 63н	Антивирусная защита	-