КАРТА РЕАЛИЗАЦИИ ТЕХНИЧЕСКИХ МЕР ПРИКАЗА № 239 ФСТЭК РОССИИ

I. Идентификация и аутентификация (ИАФ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Да	По веб-интерфейсу в браузере, MAC, IP, Ideco Agent, SSO, журнал без-ти AD
ИАФ.2	Идентификация и аутентификация устройств	Да	MAC, IP, SSO, журнал без-ти AD
ИАФ.3	Управление идентификаторами	Да	Список пользователей и управление ими через веб-интерфейс
ИАФ.4	Управление средствами аутентификации	Да	-
ИАФ.5	Идентификация и аутентификация внешних пользователей	Да	Функционал «обнаружение устр-в»
ИАФ.6	Двусторонняя аутентификация	Нет	-
ИАФ.7	Защита аутентификационной информации при передаче	Да	-

II. Управление доступом (УПД)			
Обозначение и номер меры	Описание меры	Ответ	Описание
УПД.1	Управление учётными записями пользователей	Да, частично	Список пользователей и управление ими через веб-интерфейс
УПД.2	Реализация политик управления доступа	Да	-
УПД.3	Доверенная загрузка	Нет	-
УПД.4	Разделение полномочий (ролей) пользователей	Нет	-

УПД.5	Назначение минимально необходимых прав и привилегий	Да	-
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	Да	-
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам	Да	-
УПД.8	Оповещение пользователя при успешном входе предыдущем доступе к информационной (автоматизированной) системе	Нет	-
УПД.9	Ограничение числа параллельных сеансов доступа	Да	-
УПД.10	Блокирование сеанса доступа пользователя при неактивности	Да	-
УПД.11	Управление действиями пользователей до идентификации и аутентификации	Да	-
УПД.12	Управление атрибутами безопасности	Да	-
УПД.13	Реализация защищенного удалённого доступа	Да	-
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	Да	-

III. Ограничение программной среды (ОПС)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения	Нет	-
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	Нет	-
ОПС.3	Управление временными файлами	Нет	-

IV. Защита машинных носителей информации (ЗНИ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ЗНИ.1	Учёт машинных носителей информации	Нет	-
ЗНИ.2	Управление физическим доступом к машинным носителям информации	Нет	-
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	Нет	Через средства мониторинга пользователей и устр-в
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации	Нет	-
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	Нет	-

ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	Нет	-
ЗНИ.7	Контроль подключения машинных носителей информации	Нет	-
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	Нет	-

V. Аудит безопасности (АУД)			
Обозначение и номер меры	Описание меры	Ответ	Описание
АУД.1	Инвентаризация информационных ресурсов	Нет	-
АУД.2	Анализ уязвимостей и их устранение	Да	-
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	Да	-
АУД.4	Регистрация событий безопасности	Да	-
АУД.5	Контроль и анализ сетевого трафика	Да	-
АУД.6	Защита информации о событиях безопасности	Да	-
АУД.7	Мониторинг безопасности	Да	-
АУД.8	Реагирование на сбои при регистрации событий безопасности	Да	Оповещения об ошибках и регистрирование логов ошибок
АУД.9	Анализ действий пользователей	Да	-
АУД.10	Проведение внутренних аудитов	Нет	-
АУД.11	Проведение внешних аудитов	Нет	-

VI. Антивирусная защита (АВЗ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
АВЗ.1	Реализация антивирусной защиты	Да	На периметре
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	Да	С использованием встроенного Почтового Релея
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	Нет	-
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Да	-
АВЗ.5	Использование средств антивирусной защиты различных производителей	Да	Касперский и ClamAV

VII. Предотвращение вторжений (компьютерных атак) (СОВ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
СОВ.1	Обнаружение и предотвращение компьютерных атак	Да	Обработки DDOS
СОВ.2	Обновление базы решающих правил	Да	-

VIII. Обеспечение целостности (ОЦЛ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ОЦЛ.1	Контроль целостности программного обеспечения	Да	Контроль целостности UTM

ОЦЛ.2	Контроль целостности информации	Нет	-
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему	Да	Роли доступа к Ideco UTM
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	Нет	-
ОЦЛ.5	Контроль ошибочных действий по вводу и (или) передаче информации и предупреждение пользователей об этих действиях	Нет	-
ОЦЛ.6	Обезличивание и (или) деидентификация информации	Нет	-

IX. Обеспечение доступности (ОДТ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ОДТ.1	Использование отказоустойчивых технических средств	Да	-
ОДТ.2	Резервирование средств и систем	Да	Использование кластеров и резервных копий (backups)
ОДТ.3	Контроль безотказного функционирования средств и систем	Да	-
ОДТ.4	Резервное копирование информации	Да	-
ОДТ.5	Обеспечение возможности восстановления информации	Да	Резервные копии (backups) Ideco UTM
ОДТ.6	Обеспечение возможности восстановления программного	Да	Резервные копии (backups) Ideco UTM

	обеспечения при нештатных ситуациях		
ОДТ.7	Кластеризация информационной (автоматизированной) системы	Да	Использование кластеров
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	Да	Ограничение скорости подключения отдельных пользователей

X. Защита технических средств и систем (ЗТС)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ЗТС.1	Защита информации от утечки по техническим каналам	Нет	-
ЗТС.2	Организация контролируемой зоны	Нет	-
ЗТС.3	Управление физическим доступом	Нет	-
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	Нет	-
ЗТС.5	Защита от внешних воздействий	Нет	Ограничение доступа и шифровка
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации	Нет	-

XI. Защита информационной (автоматизированной) системы и её компонентов (ЗИС)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	Да	-
ЗИС.2	Защита периметра информационной (автоматизированной) системы	Да	-
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	Да	По периметру
ЗИС.4	Сегментирование информационной (автоматизированной) системы	Да	-
ЗИС.5	Организация демилитаризованной зоны	Да	-
ЗИС.6	Управление сетевыми потоками	Да	Ограничения по пользователям и выбор маршрутов
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения («песочница»)	Нет	-
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	Да	-
ЗИС.9	Создание гетерогенной среды	Нет	-
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем	Нет	-

ЗИС.11	Предотвращение задержки или прерывания процессов с высоким приоритетом со стороны процессов с низким приоритетом	Нет	-
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти	Нет	-
ЗИС.13	Защита неизменяемых данных	Нет	-
ЗИС.14	Использование неперезаписываемых машинных носителей информации	Нет	-
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек	Нет	
ЗИС.16	Защита от спама	Да	-
ЗИС.17	Защита информации от утечек	Да	-
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещённых к использованию	Да	-
ЗИС.19	Защита информации при её передаче по каналам связи	Да	-
ЗИС.20	Обеспечение доверенных канала и маршрута	Да	-
ЗИС.21	Запрет несанкционированной удалённой активации периферийных устройств	Нет	-
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами	Да	-
ЗИС.23	Контроль использования мобильного кода	Да	-

ЗИС.24	Контроль передачи речевой информации	Да	-
ЗИС.25	Контроль передачи видеоинформации	Да	-
ЗИС.26	Подтверждение происхождения источника информации	Нет	-
ЗИС.27	Обеспечение подлинности сетевых соединений	Да	-
ЗИС.28	Исключение возможности отрицания отправки информации	Нет	-
ЗИС.29	Исключение возможности отрицания получения информации	Нет	-
ЗИС.30	Использование устройств терминального доступа	Нет	-
ЗИС.31	Защита от скрытых каналов передачи информации	Да	Расшифровка HTTPS
ЗИС.32	Защита беспроводных соединений	Да	-
ЗИС.33	Исключение доступа через общие ресурсы	Нет	-
ЗИС.34	Защита от угроз отказа в обслуживании (DOS- / DDOS-атак)	Да	-
ЗИС.35	Управление сетевыми соединениями	Да	-
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем	Нет	-
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)	Да	Кластеризация
ЗИС.38	Защита информации при использовании мобильных устройств	Да	При подключении через Ideco UTM

ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Нет	-

XII. Реагирование на компьютерные инциденты (ИНЦ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ИНЦ.1	Выявление компьютерных инцидентов	Да	-
ИНЦ.2	Информирование о компьютерных инцидентах	Да	-
ИНЦ.3	Анализ компьютерных инцидентов	Да	-
ИНЦ.4	Устранение последствий компьютерных инцидентов	Нет	-
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	Нет	-
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	Да	-

XIII. Управление конфигурацией (УКФ)			
Обозначение и номер меры	Описание меры	Ответ	Описание
УКФ.1	Идентификация объектов управления конфигурацией	Нет	-
УКФ.2	Управление изменениями	Нет	-

УКФ.3	Установка (инсталляция) только разрешённого к использованию программного обеспечения	Нет	-
УКФ.4	Контроль действий по внесению изменений	Нет	-

XIV. Управление обновлениями программного обеспечения (ОПО)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ОПО.1	Поиск и получение обновлений программного обеспечения от доверенного источника	Да	Обновления Ideco UTM
ОПО.2	Контроль целостности обновлений программного обеспечения	Да	Обновления Ideco UTM
ОПО.3	Тестирование обновлений программного обеспечения	Да	Ранний доступ к тестовым обновлениям
ОПО.4	Установка обновлений программного обеспечения	Да	Обновления Ideco UTM

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	Нет	-
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	Нет	-

XVI. Обеспечение действий в нештатных ситуациях (ДНС)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ДНС.1	Разработка плана действий в нештатных ситуациях	Нет	-
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	Нет	-
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций	Нет	-
ДНС.4	Резервирование программного обеспечения, тех. средств, каналов связи на случай возникновения нештатных ситуаций	Нет	-
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возн. нештатных ситуаций	Нет	-
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	Нет	-

XVII. Информирование и обучение персонала (ИПО)			
Обозначение и номер меры	Описание меры	Ответ	Описание
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	Нет	-
ИПО.2	Обучение персонала правилам безопасной работы	Нет	-
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы	Нет	-
ИПО.4	Контроль осведомлённости персонала об угрозах безопасности информации и о правилах безопасной работы	Нет	-