ideco

Реализация мер приказов для межсетевого экрана Ideco

Обозначения и область применения

+ — функциональные возможности Ideco NGFW могут быть использованы для реализации меры.
+/- — частичное соответствие: Ideco NGFW реализует часть требований меры; границы указаны в комментарии.
- — мера не реализуется средствами Ideco NGFW, не требуется по исходной матрице либо относится к другим классам СЗИ / организационным мерам; уточнение указано в комментарии.

Для приказа №117 знак +/- используется для мер, не являющихся обязательными для классов защищенности 1–3 и реализованных не в полном объеме.

Важно

Документ носит справочный характер и представляет сопоставление функциональных возможностей Ideco NGFW с мерами приказов ФСТЭК России №239, №21 и №117. Наличие функциональности Ideco NGFW само по себе не означает полного выполнения требований приказа или соответствия конкретной информационной системы. Состав применимых мер и способ их реализации определяются для конкретной ИС с учетом класса / уровня защищенности, модели угроз, архитектуры и организационных мер. Для сертифицированных исполнений применимость функциональности определяется областью действия сертификата и эксплуатационной документацией.

Для приказа №117 оценка относится к применимости функциональности Ideco FSTEC 21 в составе комплексной системы защиты. Знак «-» не означает невозможность выполнения меры в информационной системе в целом.

Реализация мер приказа №239
Межсетевой экран Ideco

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		3	2	1		
I. Идентификация и аутентификация (ИАФ)						
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	+	+	+	-	Сторонние СЗИ / организационные меры
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+	+	При парольной аутентификации без 2FA требуются срок действия пароля не более 90 дней и запрет повторного использования
ИАФ.2	Идентификация и аутентификация устройств	+	+	+	+	Аутентификация и идентификация по IP и MAC + Ideco Client с ZTNA и HIP
ИАФ.3	Управление идентификаторами	+	+	+	+	
ИАФ.4	Управление средствами аутентификации	+	+	+	+	
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+	+/-	ГОСТ VPN
ИАФ.6	Двусторонняя аутентификация				+	Цифровые сертификаты
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+	+	
II. Управление доступом (УПД)						
УПД.0	Регламентация правил и процедур управления доступом	+	+	+	-	Сторонние СЗИ / организационные меры
УПД.1	Управление учетными записями пользователей	+	+	+	+/-	Централизованное управление учетными записями (административные и пользовательские)
УПД.2	Реализация модели управления доступом	+	+	+	+	
УПД.3	Доверенная загрузка		+	+	+	Модуль доверенной загрузки есть не во всех платформах МЭ
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+	+	
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+	+	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+	+/-	Требуются автоматическая блокировка/удаление временных и неиспользуемых учетных записей и разблокировка учетной записи администратора только другим администратором
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				-	Не требуется по матрице
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				-	Не требуется по матрице
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	+	+	+	+	Закрывается обычным VPN
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+	+	
III. Ограничение программной среды (ОПС)						
ОПС.0	Регламентация правил и процедур ограничения программной среды		+	+	-	Сторонние СЗИ / организационные меры
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+	-	Сторонние СЗИ / организационные меры
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+	-	Сторонние СЗИ / организационные меры
ОПС.3	Управление временными файлами				-	Сторонние СЗИ / организационные меры
IV. Защита машинных носителей информации (ЗНИ)						
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	+	+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.1	Учет машинных носителей информации	+	+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+	+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				-	Сторонние СЗИ / организационные меры
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				-	Сторонние СЗИ / организационные меры
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	+	+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации			+	-	Сторонние СЗИ / организационные меры
ЗНИ.7	Контроль подключения съемных машинных носителей информации	+	+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+	+	+	-	Сторонние СЗИ / организационные меры
V. Аудит безопасности (АУД)						
АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+	-	Сторонние СЗИ / организационные меры
АУД.1	Инвентаризация информационных ресурсов	+	+	+	-	Сторонние СЗИ / организационные меры
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	+	+	+	-	Сторонние СЗИ / организационные меры
АУД.11	Проведение внешних аудитов				-	Сторонние СЗИ / организационные меры
VI. Антивирусная защита (АВЗ)						
АВЗ.0	Регламентация правил и процедур антивирусной защиты	+	+	+	-	Сторонние СЗИ / организационные меры
АВЗ.1	Реализация антивирусной защиты	+	+	+	+	
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+	+/-	Антивирус и антиспам для почты
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			+	+/-	Использование антивирусов различных производителей
VII. Предотвращение вторжений (компьютерных атак) (СОВ)						
СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)		+	+	-	Сторонние СЗИ / организационные меры
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+	+	
СОВ.2	Обновление базы решающих правил		+	+	+	

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		3	2	1		
VIII. Обеспечение целостности (ОЦЛ)						
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	+	+	+	-	Сторонние СЗИ / организационные меры
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+	+	Есть контроль целостности самого МЭ + необходимо проверять целостность стороннего ПО сторонними СЗИ и организационными мерами
ОЦЛ.2	Контроль целостности информации				-	Сторонние СЗИ / организационные меры
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+	+	Ролевая система доступа + DLP системы
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+	-	Сторонние СЗИ / организационные меры
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+	-	Сторонние СЗИ / организационные меры
ОЦЛ.6	Обезличивание и (или) деидентификация информации				-	Сторонние СЗИ / организационные меры
IX. Обеспечение доступности (ОДТ)						
ОДТ.0	Регламентация правил и процедур обеспечения доступности	+	+	+	-	Сторонние СЗИ / организационные меры
ОДТ.1	Использование отказоустойчивых технических средств		+	+	+	
ОДТ.2	Резервирование средств и систем		+	+	+	Кластеризация, бэкапы
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+	+	Кластеризация, бэкапы
ОДТ.4	Резервное копирование информации	+	+	+	+	Бэкапы
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+	+	Бэкапы
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+	+	Бэкапы
ОДТ.7	Кластеризация информационной (автоматизированной) системы				+	Кластеризация, бэкапы
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+	+	Ограничение скорости для отдельных пользователей
X. Защита технических средств и систем (ЗТС)						
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.1	Защита информации от утечки по техническим каналам				-	Сторонние СЗИ / организационные меры
ЗТС.2	Организация контролируемой зоны	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.3	Управление физическим доступом	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.5	Защита от внешних воздействий	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации				-	Сторонние СЗИ / организационные меры
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)						
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	+	+	+	-	Не касается СЗИ. Внутренние регламенты компании
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+	+	В Изделии реализована ролевая система доступа
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	+	+	+	+	DMZ сети
ЗИС.6	Управление сетевыми потоками	+	+	+	+	
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				+	Должно реализовываться сторонними СЗИ
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+	+	
ЗИС.9	Создание гетерогенной среды				-	Сторонние СЗИ / организационные меры
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				-	Сторонние СЗИ / организационные меры
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				-	Сторонние СЗИ / организационные меры
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				-	Сторонние СЗИ / организационные меры
ЗИС.13	Защита неизменяемых данных		+	+	-	Сторонние СЗИ / организационные меры
ЗИС.14	Использование неперезаписываемых машинных носителей информации				-	Сторонние СЗИ / организационные меры
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				+	
ЗИС.16	Защита от спама		+	+	+/-	Модули антиспама
ЗИС.17	Защита информации от утечек				-	DLP
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	+	+	+	-	Сторонние СЗИ / организационные меры
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				-	ГОСТ VPN с проверкой политик на уровне метаданных
ЗИС.23	Контроль использования мобильного кода				+	Закрывается Контролем приложений
ЗИС.24	Контроль передачи речевой информации				-	DLP
ЗИС.25	Контроль передачи видеоинформации				-	DLP
ЗИС.26	Подтверждение происхождения источника информации				-	ЭЦП
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+	+	
ЗИС.28	Исключение возможности отрицания отправки информации				-	Сторонние СЗИ / организационные меры
ЗИС.29	Исключение возможности отрицания получения информации				-	Сторонние СЗИ / организационные меры
ЗИС.30	Использование устройств терминального доступа				+	Терминальный агент
ЗИС.31	Защита от скрытых каналов передачи информации				+	Расшифровка HTTPs
ЗИС.32	Защита беспроводных соединений	+	+	+	+	Возможность авторизации устройств раздачи беспроводного Интернета и их контроль
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				-	Сторонние СЗИ / организационные меры
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				+	Кластеризация, бэкапы
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+	-	Сторонние СЗИ / организационные меры
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+	-	Сторонние СЗИ / организационные меры

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		3	2	1		
XII. Реагирование на компьютерные инциденты (ИНЦ)						
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	+	+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.1	Выявление компьютерных инцидентов	+	+	+	+	
ИНЦ.2	Информирование о компьютерных инцидентах	+	+	+	+	
ИНЦ.3	Анализ компьютерных инцидентов	+	+	+	+	
ИНЦ.4	Устранение последствий компьютерных инцидентов	+	+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	+	+	+	+	
XIII. Управление конфигурацией (УКФ)						
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	+	+	+	-	Сторонние СЗИ / организационные меры
УКФ.1	Идентификация объектов управления конфигурацией				+	Все администраторы должны пройти аутентификацию и идентификацию перед изменением конфигураций сети Уточнение: пункт касается не только МЭ, но и всей инфраструктуры в целом
УКФ.2	Управление изменениями	+	+	+	+	Есть возможность просмотра логов с изменениями в конфигурации Уточнение: пункт касается не только МЭ, но и всей инфраструктуры в целом
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+	-	Сторонние СЗИ / организационные меры
УКФ.4	Контроль действий по внесению изменений				+	В МЭ есть контроль целостности ПО и настроек с набором правил. Пункт касается не только МЭ, но и всей инфраструктуры в целом
XIV. Управление обновлениями программного обеспечения (ОПО)						
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	+	+	+	-	Сторонние СЗИ / организационные меры
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+	+	Обновление МЭ происходит либо через доверенные каналы с нашим сервером, либо посредством оффлайн обновлений с внешних носителей информации. Обновление стороннего ПО в ИС также должно контролироваться
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+	+	Есть контроль целостности самого межсетевого экрана. Также должен быть реализован контроль целостни стороннего ПО при помощи сторонних СЗИ или организационных мер
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+	-	Сторонние СЗИ / организационные меры
ОПО.4	Установка обновлений программного обеспечения	+	+	+	-	Сторонние СЗИ / организационные меры
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)						
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	+	+	+	-	Сторонние СЗИ / организационные меры
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+	+	+	-	Сторонние СЗИ / организационные меры
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+	-	Сторонние СЗИ / организационные меры
XVI. Обеспечение действий в нештатных ситуациях (ДНС)						
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	+	+	+	-	Сторонние СЗИ / организационные меры
ДНС.1	Разработка плана действий в нештатных ситуациях	+	+	+	-	Сторонние СЗИ / организационные меры
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+	-	Сторонние СЗИ / организационные меры
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+	-	Сторонние СЗИ / организационные меры
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+	-	Сторонние СЗИ / организационные меры
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+	+	+	+	Есть возможность восстановить функционирование МЭ. Пункт касается не только МЭ, но и всей инфраструктуры в целом
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+	-	ИБ отдел, SIEM, SOAR
XVII. Информирование и обучение персонала (ИПО)						
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	+	+	+	-	Сторонние СЗИ / организационные меры
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	-	Сторонние СЗИ / организационные меры
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+	-	Сторонние СЗИ / организационные меры
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+	-	Сторонние СЗИ / организационные меры
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+	-	Сторонние СЗИ / организационные меры

Реализация мер приказа №117

Межсетевой экран Ideco

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		1	2	3		
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)						
ИАФ.1	Идентификация пользователей	+	+	+	+	
ИАФ.2	Идентификация устройств				+	
ИАФ.3	Аутентификация пользователей	+	+	+	-	Аутентификация реализована; политика паролей и блокировка УЗ — внешний каталог/IAM/IdM и оргмеры
ИАФ.4	Аутентификация устройств				+	
Управление доступом субъектов доступа к объектам доступа (УПД)						
УПД.1	Реализация модели управления доступом	+	+	+	+	
УПД.2	Разграничение и контроль прав доступа	+	+	+	+	
УПД.3	Управление учетными записями	+	+	+	-	Учетные записи используются в политиках; полный жизненный цикл УЗ — внешний каталог/IAM/IdM и оргмеры
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+	+	-	Контроль и журналирование попыток доступа реализованы; управление временными/неиспользуемыми УЗ и разблокировка — внешний каталог/IAM/IdM и оргмеры
УПД.5	Предупреждение пользователя при его доступе к информационной системе				+/-	Мера не обязательна для классов 1–3
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему				+/-	Мера не обязательна для классов 1–3
УПД.7	Ограничение числа параллельных сеансов доступа	+	+		+	
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+	+	+	+	
УПД.9	Контроль действий субъектов доступа до идентификации и аутентификации	+	+	+	+	
Регистрация событий безопасности (РСБ)						
РСБ.1	Определение событий безопасности и данных о них, подлежащих регистрации	+	+	+	+	
РСБ.2	Анализ событий безопасности и реагирование на них	+	+	+	+	Интеграция с SIEM для расширенного анализа и корреляции
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+	+	
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+	+	+	
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+	+	
Защита виртуализации и облачных технологий (ЗСВ)						
ЗСВ.1	Доверенная загрузка средств виртуализации и виртуальных машин	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.2	Контроль целостности средств виртуализации и виртуальных машин	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.3	Регистрация событий безопасности в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.4	Управление доступом в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.5	Резервное копирование в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.6	Ограничение программной среды в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.7	Защита памяти в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.8	Идентификация и аутентификация в среде виртуализации	+	+	+	-	Платформа виртуализации / специализированные СЗИ виртуализации
ЗСВ.9	Управление виртуальными машинами	+	+		-	Платформа виртуализации / специализированные СЗИ виртуализации

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		1	2	3		
Защита технологий контейнерных сред и их оркестрации (ЗКО)						
ЗКО.1	Контроль целостности в контейнерных средах	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.2	Регистрация событий безопасности в контейнерных средах	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.3	Управление доступом в контейнерных средах	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.4	Резервное копирование в контейнерных средах	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.5	Изоляция контейнеров в контейнерной среде	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.6	Идентификация и аутентификация в контейнерной среде	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.7	Управление контейнерами и их образами	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
ЗКО.8	Выявление и устранение уязвимостей в контейнерной среде	+	+	+	-	Контейнерная платформа / оркестратор / специализированные СЗИ
Защита сервисов электронной почты (ЗЭП)						
ЗЭП.1	Защита ящиков и сообщений электронной почты	+	+	+	+	
ЗЭП.2	Контроль доступа пользователей	+	+	+	+	
ЗЭП.3	Защита от вредоносных вложений	+	+	+	-	Сторонние СЗИ антивирусной защиты почты
ЗЭП.4	Защита от фишинга	+	+	+	-	Сторонние СЗИ защиты почты / оргмеры; DMARC, DKIM, SPF
ЗЭП.5	Защита от спама	+	+	+	-	Сторонние СЗИ защиты почты / антиспам
ЗЭП.6	Защита метаданных и иной технической информации сервисов электронной почты	+	+	+	-	Почтовая система / специализированные СЗИ защиты почты
Защита веб-технологий (ЗВТ)						
ЗВТ.1	Защита пользовательских данных	+	+	+	+	
ЗВТ.2	Контроль доступа пользователей	+	+	+	+	
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+	+	+	-	Требуется проверка API по спецификации (ЗПИ.3)
ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+	+	
ЗВТ.5	Проверка файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение	+	+	+	-	Сторонние СЗИ проверки файлов; Ideco — контроль доступа, WAF и журналирование
Защита программных интерфейсов взаимодействия приложений (API), (ЗПИ)						
ЗПИ.1	Защита данных API	+	+	+	+	
ЗПИ.2	Контроль доступа пользователей и приложений	+	+	+	+	
ЗПИ.3	Проверка на соответствие спецификации API	+	+	+	-	Проверка API-запросов по спецификации не реализована
Защита конечных устройств (ЗКУ)						
ЗКУ.1	Управление доступом к конечным устройствам	+	+	+	+	
ЗКУ.2	Обеспечение целостности программного обеспечения конечного устройства	+	+	+	-	Сторонние СЗИ конечных устройств / контроль целостности
ЗКУ.3	Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах	+	+	+	-	Сторонние СЗИ конечных устройств / антивирус / EDR.
ЗКУ.4	Мониторинг процессов и состояния устройства	+	+	+	-	Мониторинг локальных процессов и состояния ОС — EDR / средства управления конечными устройствами
ЗКУ.5	Контроль и фильтрация трафика на конечном устройстве				-	Сторонние СЗИ конечных устройств / локальная фильтрация трафика
ЗКУ.6	Анализ и реагирование на события безопасности	+	+	+	-	Ideco формирует сетевые события; реагирование на конечном устройстве — EDR / SIEM / SOAR

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		1	2	3		
Защита мобильных устройств (ЗМУ)						
ЗМУ.1	Идентификация и аутентификация пользователей	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.2	Управление доступом пользователей к мобильным устройствам	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.3	Обеспечение целостности	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.4	Защита данных	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.5	Антивирусная защита	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.6	Контроль приложений	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.7	Ограничение и контроль функциональности	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.8	Определение и контроль геопозиции				-	MDM/EMM / специализированные СЗИ мобильных устройств
ЗМУ.9	Регистрация, анализ и реагирование на события безопасности	+	+	+	-	MDM/EMM / специализированные СЗИ мобильных устройств
Защита технологий «интернета вещей» (ЗИВ)						
ЗИВ.1	Идентификация и аутентификация	+	+	+	-	Требование в полном объеме не реализовано, в том числе в части специализированных протоколов и механизмов управления IoT-устройствами
ЗИВ.2	Управление доступом	+	+	+	-	Требование в полном объеме не реализовано
ЗИВ.3	Защита данных	+	+	+	-	Требование в полном объеме не реализовано
ЗИВ.4	Контроль целостности	+	+	+	-	IoT-платформа / специализированные СЗИ контроля целостности
ЗИВ.5	Регистрация, анализ и реагирование на события безопасности	+	+	+	-	Требование в полном объеме не реализовано
Защита точек беспроводного доступа (ЗБД)						
ЗБД.1	Идентификация и аутентификация	+	+	+	+	
ЗБД.2	Управление доступом	+	+	+	+	
ЗБД.3	Защита пользовательских данных	+	+	+	+	
ЗБД.4	Контроль целостности	+	+	+	-	Беспроводная инфраструктура / специализированные СЗИ контроля целостности
ЗБД.5	Ограничение уровней сигналов	+	+	+	-	Точки доступа / WLAN-контроллеры
ЗБД.6	Регистрация, анализ и реагирование на события безопасности	+	+	+	-	Беспроводная инфраструктура / системы сбора и анализа событий
Антивирусная защита (АВЗ)						
АВЗ.1	Антивирусная защита устройств	+	+	+	-	Сторонние СЗИ антивирусной защиты конечных устройств
АВЗ.2	Антивирусная защита электронной почты	+	+	+	-	Сторонние СЗИ антивирусной защиты почты
АВЗ.3	Антивирусная проверка сетевого трафика	+	+	+	-	Сторонние СЗИ антивирусной проверки сетевого трафика
АВЗ.4	Применение замкнутой системы (среды) предварительного выполнения программ («песочницы»)				+	
Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)						
СОВ.1	Обнаружение и предотвращение вторжений на периметреита устройств	+	+	+	+	
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы	+	+	+	+	
Сегментация и межсетевое экранирование (МСЭ)						
МСЭ.1	Сегментация сети	+	+	+	+	
МСЭ.2	Организация демилитаризованной зоны	+	+	+	+	
МСЭ.3	Контроль сетевого доступа и фильтрация трафика	+	+	+	+	
МСЭ.4	Маскирование системы				-	NAT и ограничение сетевой видимости; полное выполнение — архитектура публикации, reverse proxy/ WAF и оргмеры
МСЭ.5	Создание ложных систем				-	Специализированные средства honeypot/honeynet

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Классы защищенности информационной системы			Наличие	Комментарий
		1	2	3		
Защита от атак, направленных на отказ в обслуживании (ЗОО)						
ЗОО.1	Защита от атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой	+	+	+	+	
ЗОО.2	Контроль и фильтрация входящего трафика	+	+	+	+	
ЗОО.3	Мониторинг состояния сервисов и интерфейсов	+	+	+	-	Ideco: мониторинг NGFW и интерфейсов; прикладные сервисы и внешние каналы — системы мониторинга
ЗОО.4	Балансировка нагрузки	+	+	+	+	
ЗОО.5	Ограничение нагрузки	+	+	+	-	Ideco: ограничение нагрузки средствами МЭ/IPS/WAF; для rate limiting, DNS и объемных атак — DNS-защита, API Gateway, балансировщик или Anti-DDoS
ЗОО.6	Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях	+	+	+	+	Требует проектирования каналов и аппаратного запаса ресурсов
Защита каналов связи и сетевого взаимодействия (ЗКС)						
ЗКС.1	Защита данных при передаче по каналам связи	+	+	+	+	
ЗКС.2	Контроль атрибутов безопасности при сетевом взаимодействии	+	+	+	+	
ЗКС.3	Обеспечение подлинности сетевых соединений	+	+	+	+	
ЗКС.4	Контроль доступа к внешним ресурсам	+	+	+	+	
ЗКС.5	Контекстная проверка исходящего трафика				-	Контент исходящего трафика — DLP; Ideco — сетевые ограничения и интеграция

Реализация мер приказа №21
Межсетевой экран Ideco

Приказ №21

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Наличие	Комментарий
		4	3	2	1		
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)							
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+	+/-	При парольной аутентификации без 2FA требуются срок действия пароля не более 90 дней и запрет повторного использования
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+	+	Аутентификация и идентификация по IP и MAC + Ideco Client с ZTNA и HIP
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+	+	Управление учетными записями пользователей
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	+	+	+	+	+	Создание, редактирование и удаление пользователей и их прав
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+	+	Защита канала связи, сокрытие вводимой информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+	+	Интеграция с внешними каталогами
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	+	+	+	+	+/-	Централизованное управление учетными записями (административные и пользовательские)
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+	+	
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)	+	+	+	+	+/-	Требуются автоматическая блокировка/удаление временных и неиспользуемых учетных записей и разблокировка учетной записи администратора только другим администратором.
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных					-	Не требуется по матрице
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему					-	Не требуется по матрице
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.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					-	Сторонние СЗИ / организационные меры
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+	+	Закрывается обычным VPN
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+	-	MDM
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+	-	MDM
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+	+	
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+	+	Есть, но не во всех аппаратных платформах
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					-	Сторонние СЗИ / организационные меры
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			+	+	-	Сторонние СЗИ / организационные меры
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+	-	Сторонние СЗИ / организационные меры
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов					-	Сторонние СЗИ / организационные меры
IV. Защита машинных носителей персональных данных (ЗНИ)							
ЗНИ.1	Учет машинных носителей персональных данных			+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+	-	Сторонние СЗИ / организационные меры
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны					-	Сторонние СЗИ / организационные меры
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах					-	Сторонние СЗИ / организационные меры
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных					-	Сторонние СЗИ / организационные меры
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных					-	Сторонние СЗИ / организационные меры
ЗНИ.7	Контроль подключения машинных носителей персональных данных					-	Сторонние СЗИ / организационные меры
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		+	+	+	-	Сторонние СЗИ / организационные меры
V. Регистрация событий безопасности (РСБ)							
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+	+	Возможность выгружать отчеты с интересующими нас событиями безопасности, настроить сроки хранения пока нет возможности. Происходит архивация всех логов
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+	+	
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+	+	
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			+	+	+	Через веб-интерфейс
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе					+	
РСБ.7	Защита информации о событиях безопасности	+	+	+	+	+	Архивация логов
VI. Антивирусная защита (АВЗ)							
АВЗ.1	Реализация антивирусной защиты	+	+	+	+	+	
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+	+	

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Наличие	Комментарий
		4	3	2	1		
VII. Обнаружение вторжений (СОВ)							
СОВ.1	Обнаружение вторжений			+	+	+	
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		+	+	+	-	Сторонние СЗИ / организационные меры
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+	-	Сторонние СЗИ / организационные меры
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+	+	Есть проверка корректности настройки МЭ, работоспособности модулей. Пункт касается всей ИС, а не только МЭ
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+	-	Сторонние СЗИ / организационные меры
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе			+	+	-	Сторонние СЗИ / организационные меры
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)							
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+	+	Есть проверка контрольных сумм исполняемых файлов, а также настроек и правил фильтрации
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы					-	Сторонние СЗИ / организационные меры
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций					+	Бэкапы. Пункт касается всей ИС, а не только МЭ
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)			+	+	+/-	Модуль антиспам
ОЦЛ.5	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					-	Сторонние СЗИ / организационные меры
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему					-	Сторонние СЗИ / организационные меры
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему					-	Сторонние СЗИ / организационные меры
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях					-	Сторонние СЗИ / организационные меры
X. Обеспечение доступности персональных данных (ОДТ)							
ОДТ.1	Использование отказоустойчивых технических средств					-	Сторонние СЗИ / организационные меры
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы					-	Сторонние СЗИ / организационные меры
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+	-	Сторонние СЗИ / организационные меры
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+	-	Сторонние СЗИ / организационные меры
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+	-	Сторонние СЗИ / организационные меры
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	+	+	+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры					-	Сторонние СЗИ / организационные меры
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией					-	Сторонние СЗИ / организационные меры
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+	-	Сторонние СЗИ / организационные меры
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+	-	Сторонние СЗИ / организационные меры
XII. Защита технических средств (ЗТС)							
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам					-	Сторонние СЗИ / организационные меры
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования					-	Сторонние СЗИ / организационные меры
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	+	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+	-	Сторонние СЗИ / организационные меры
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)					-	Сторонние СЗИ / организационные меры

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных				Наличие	Комментарий
		4	3	2	1		
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 персональных данных, функций по обработке персональных данных и иных функций информационной системы				+	+	Ролевая система доступа
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом					-	Сторонние СЗИ / организационные меры
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	+	+	+	+	+/-	ГОСТ VPN
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)					-	ГОСТ VPN
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств					-	Сторонние СЗИ / организационные меры
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами					-	Сторонние СЗИ / организационные меры
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					-	Сторонние СЗИ / организационные меры
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					-	Сторонние СЗИ / организационные меры
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					-	Сторонние СЗИ / организационные меры
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 персональных данных другому пользователю					-	Сторонние СЗИ / организационные меры
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя					-	Сторонние СЗИ / организационные меры
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных					-	Сторонние СЗИ / организационные меры
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+	-	Сторонние СЗИ / организационные меры
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов					-	Сторонние СЗИ / организационные меры
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+	+	Сегментирование, VLAN
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения					-	Сторонние СЗИ / организационные меры
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти					-	Сторонние СЗИ / организационные меры
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+	+	Возможность авторизации устройств раздачи беспроводного Интернета и их контроль
XIV. Выявление инцидентов и реагирование на них (ИНЦ)							
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+	-	Сторонние СЗИ / организационные меры
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+	-	Сторонние СЗИ / организационные меры
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		+	+	+	-	Сторонние СЗИ / организационные меры
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+	+	Есть возможность просмотра логов с изменениями в конфигурации. Пункт касается не только МЭ, но и всей инфраструктуры в целом
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		+	+	+	+	Есть проверка корректности работы правил. Пункт касается не только МЭ, но и всей инфраструктуры в целом
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+	+	Можно посмотреть историю изменения правил. Пункт касается не только МЭ, но и всей инфраструктуры в целом