# ОБЗОР ВОЗМОЖНОСТЕЙ МЕЖСЕТЕВОГО ЭКРАНА IDECO UTM

| СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ | |
|---|---|
| Сертификация ФСТЭК: Межсетевой экран, Система обнаружения вторжений | Номер сертификата 4503, срок действия 28.12.2026. Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ). |
| Тип и класс ИС (для защиты которых подходит) | ГИС: до 1 КЗ (включительно),<br>ИСПДн: до 1 УЗ (включительно),<br>АСУ: до К1 (включительно),<br>Значимые объекты КИИ: до 1 класса (включительно), ИС<br>ОП: II класс. |
| Законы, регламентирующие применение | 187-ФЗ «О безопасности КИИ РФ»,<br>152-ФЗ «О персональных данных»,<br>139-ФЗ и 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". |

| ИНТЕГРАЦИЯ В ИС | |
|---|---|
| На периметре сети | Тип МЭ А (сертифицированный ПАК). |
| Между сегментами локальной сети | Тип МЭ Б (ПО)<br>Возможно использование собственного железа или виртуальной машины. |
| Прокси-сервер | Тип МЭ Б (ПО)<br>Возможно использование собственного железа или виртуальной машины. |

| ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ | |
|---|---|
| Межсетевой экран | Защищает корпоративную сеть от атак извне. Правила можно применять как для всей сети и отдельных подсетей, так и для отдельных пользователей или групп, даже если у них используются динамические IP-адреса. Предустановленные правила позволяют обеспечить высокий уровень защиты, даже без специальной настройки. |
| Система предотвращения вторжений IDS/IPS | Система обнаружения и предотвращения вторжений блокирует попытки несанкционированного доступа, эксплойты, ботнеты, DoS-атаки, вирусную активность в сети, spyware, TOR, анонимайзеры, телеметрию Windows и скомпрометированные IP-адреса (с помощью обновляемой базы IP Reputation).<br>Ведет журналирование инцидентов информационной безопасности. |

| | |
|---|---|
| Контроль приложений | Возможность управлять доступом к различным приложениям: Skype, мессенджерам, torrent-клиентам и другим (более 250 приложений). |
| Защита от подбора паролей к сервисам brute force | Специальная служба блокирует brute force атаки (попытки подбора паролей и многократные подключения к сервисам) на сервисы SSH, SMTP, IMAP, POP3, вебпочту, VPN-сервер и доступ в административный веб-интерфейс UTM. |
| **ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ОТ ВНЕШНИХ И ВНУТРЕННИХ УГРОЗ** | |
| Интеграция с внешними решениями | Возможность интеграции по протоколу ICAP со сторонними DLP-системами, антивирусами и решениями для контентной фильтрации. Интеграция с SIEM (по протоколу syslog), с системами мониторинга (SNMP, Zabbix-агент). |

| | |
|---|---|
| **КОНТРОЛЬ ДОСТУПА** | |
| Active Directory / LDAP | Возможность синхронизации и авторизации пользователей через Active Directory и LDAP сервер. Поддержка интеграции с несколькими доменами Active Directory. |
| Авторизация пользователей Identity-Based Control | Авторизация по логину и паролю через VPN, PPPoE, авторизация по IP-адресу и по MAC-адресу, через веб-браузер, прозрачная Single Sign-On аутентификация по Kerberos/NTLM, по логам безопасности контроллеров домена через Active Directory.<br>Доступ к Интернету неавторизованных устройств блокируется сервером. |
| Отчеты | Модуль формирования отчетов для руководителей и IT-менеджеров, позволяющий визуально оценивать степень использования Интернет-ресурсов сотрудниками и подразделениями компании. |

| | |
|---|---|
| **УДАЛЕННЫЕ ПОДКЛЮЧЕНИЯ (VPN-СЕРВЕР)** | |
| Удаленные офисы и филиалы \ протоколы site-to-site VPN | Поддерживаются протоколы: IKEv2 IPSec, L2TP/IPSec, SSTP. |
| Мобильные сотрудники \ протоколы client-to-site VPN | До 1000 одновременных сессий. IKEv2 IPSec, L2TP/IPSec, SSTP, PPTP. |

| | |
|---|---|
| Расширенный контентфильтр | 146 категорий, более 500 млн url в обновляемой базе данных.<br>Используются базы российского производителя баз фильтрации с высокой степенью релевантности для русскоязычного интернет-сегмента. |
| Декодирование и проверка HTTPSтрафика | SSL bump, либо фильтрация без подмены сертификата с помощью SNI и анализа данных сертификата. |
| Блокировка файлов | Контент-фильтр позволяет блокировать трафик по типу (MIME-type) и расширению файлов. |

| УПРАВЛЕНИЕ ТРАФИКОМ | |
|---|---|
| Маршрутизация трафика | Поддерживаются виртуальные 802.1q VLAN интерфейсы, PPTP, L2TP, PPPoE интерфейсы. Возможность указать маршруты по источнику. |
| Подключение к провайдерам, резервирование и балансировка каналов | Поддержка нескольких каналов провайдеров и нескольких внешних сетей;<br>Перенаправление трафика в разные подсети;<br>Балансировка трафика между несколькими интернет-каналами;<br>Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера, в случае необходимости.<br>Подключение к провайдеру по протоколам PPTP (VPN), L2TP и PPPoE. |
| **УПРАВЛЕНИЕ ТРАФИКОМ** | |
| Управление полосой пропускания | Интернет-канала для пользователей и групп. |
| Кэширование трафика и DNS-запросов | Встроенный прокси-сервер кэширует трафик популярных ресурсов для ускорения доступа к ним. DNS-сервер кэширует DNS-запросы, что также позволяет ускорить доступ к Интернет-ресурсам. |
| Публикация ресурсов Reverse Proxy, DNAT, SMTP relay | Возможна публикация веб-ресурсов с помощью обратного прокси (Reverse Proxy).<br>Поддерживается публикация Outlook Web Access.<br>Публикация ресурсов с помощью переадресации портов (DNAT).<br>Публикация почтового сервера с помощью почтового релея позволяет использовать все возможности фильтрации почтового трафика на Ideco UTM и защитить внутренний почтовый сервер от атак и спама. |
| **КОНТЕНТНАЯ ФИЛЬТРАЦИЯ** | |

| ХАРАКТЕРИСТИКИ АППАРАТНОЙ ПЛАТФОРМЫ (СЕРТИФИКАТ ПО ТИПУ А) Ideco MX ФСТЭК | |
|---|---|
| Форм-фактор | 1U. 44/438/321 мм |
| Процессор | Intel Atom C3758 (8 ядер, 2,2 ГГц, 16 МБ кэш, 25 Вт) |
| Оперативная память | 16 Gb DDR4 |
| Хранилище | SSD 240Gb SATA |
| Сетевые интерфейсы | 100/1000 – 8 шт. |

| ПОЧТОВЫЙ РЕЛЕЙ | |
|---|---|
| Режим работы | Полноценный почтовый сервер или почтовый релей для фильтрации почтового трафика. |
| Поддержка протоколов | Поддержка протоколов IMAP, POP3, SMTP. Шифрованных протоколов POP3S, IMAPS, STARTTLS - все они используются с максимально криптостойкими алгоритмами шифрования. |
| Веб-интерфейс | Веб-интерфейс почтового сервера обеспечивает безопасный удаленный доступ пользователей к почте.<br>В пользовательском интерфейсе также присутствует общая и пользовательская адресные книги, календари событий и задач. |
| Антиспам | Фильтрация спама с помощью сервисов DNS blacklist.<br>Предварительный спам-фильтр защищает почтовый сервер от подключений ботов, спама и DoS-атак. Проверяет соответствие SPF-записи и корректность DKIMподписи сервера. |

| РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ | |
|---|---|
| Отказоустойчивая конфигурация | Кластер отказоустойчивости (Active-Passive). Входит в стандартную лицензию. |
| WEB-интерфейс | Полное управление сервером и конфигурирование через WEB-браузер. |
| Консольный интерфейс | Возможно удаленное подключение к серверу по SSH и выполнение консольных команд. |
| Active Directory / LDAP | Интеграция с каталогами пользователей и ресурсов компании. |

| ХАРАКТЕРИСТИКИ АППАРАТНОЙ ПЛАТФОРМЫ (СЕРТИФИКАТ ПО ТИПУ А) Ideco MX ФСТЭК | |
|---|---|
| Производительность фильтрации интернеттрафика | В режиме L3 FW: 1 Гбит/с<br>В режиме контент-фильтра: до 750 Мбит/с<br>В режиме UTM (FW, IPS, CF, AC): до 150 Мбит/с |
| Количество пользователей | От 100 до 350 |
| Поставка | Есть в наличии, поставка в течении 2-х недель. |

| ХАРАКТЕРИСТИКИ АППАРАТНОЙ ПЛАТФОРМЫ (СЕРТИФИКАТ ПО ТИПУ А) Ideco MX+ ФСТЭК | |
|---|---|
| Форм-фактор | 1U. 44/438/321 мм |
| Процессор | Intel Atom C3958 (16 ядер, 2 ГГц, 16 МБ кэш, 31 Вт) |
| Оперативная память | 16 Gb DDR4 |
| Хранилище | SSD 240Gb SATA |
| Сетевые интерфейсы | 100/1000 – 8 шт. |
| Производительность фильтрации интернеттрафика | В режиме L3 FW: 1 Гбит/с<br>В режиме контент-фильтра: до 900 Мбит/с<br>В режиме UTM (FW, IPS, CF, AC): до 250 Мбит/с |
| Количество пользователей | От 250 до 600 |
| Поставка | Предзаказ, начало поставок с 20.06.2022 (ориентировочно). |

| ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ | |
|---|---|
| Приобретение и поставка программного обеспечения | Неисключительное право на использование программного продукта Ideco UTM приобретаются у правообладателя и включают в себя доступ к обновлениям ПО и технической поддержке сроком на 1 год. |
| Срок действия лицензии на ПО | Лицензия на неисключительные права доступа действует бессрочно с даты покупки. |

| | |
|---|---|
| Подписка на обновления и техническую поддержку (Security Update) | Security Update включает в себя:<br>- Получение новых версий продукта (обновлений Ideco UTM).<br>- Базы данных расширенного контент-фильтра (обновления баз и их работа). - Систему предотвращения вторжений (обновления баз модуля и возможность его работы).<br>- Контроль приложений (обновления модуля и возможность его работы).<br>- Техническую поддержку.<br>Модули системы предотвращения вторжений, контроль приложений - работают только при активной подписке.<br><br>Льготное продление Security Update.<br>Стоимость покупки модуля составляет 45% от текущих прайсовых цен на продукт.<br><br>Вы можете приобрести Security Update на этих условиях в течение двух месяцев с момента завершения срока активности обновлений и технической поддержки. Срок |
| **ЖИЗНЕННЫЙ ЦИКЛ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** | |
| | активности Security Update продлевается ровно на один год с момента завершения предыдущего периода.<br><br>Позднее продление Security Update.<br>Независимо от даты окончания активности Security Update (если прошло больше двух месяцев) вы можете приобрести его за 75% базовой цены вашей редакции.<br><br>Срок активности Security Update продлевается с момента оплаты ровно на один год. Вы получаете возможность загрузить и установить все изменения и обновления, которые вышли за весь предыдущий период, пока вы не пользовались обновлениями и еще в течение полного года с момента покупки пользоваться поддержкой, обновлениями продукта и UTM-модулями. |
| Прямая техническая поддержка от вендора | Техническая поддержка ПО, включающая помощь пользователям в настройки и эксплуатации системы, а также устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, осуществляется службой технической поддержки компании.<br><br>Поддержка осуществляется в соответствии с утвержденным регламентом. Эскалация обращений происходит до уровня разработчиков ПО.<br><br>Поддержка доступна в тикетной системе обращений и по телефону, с 7 до 19 часов по Московскому времени в рабочие дни и с 9 до 16 по субботам. |
| Документация | Руководство администратора сервера Ideco UTM. |

## Реализация мер защиты КИИ и ИСПДн

| |
|---|
| **Реализация мер защиты КИИ (по приказу ФСТЭК №235 от 21.12.2017)** |

| Требуемые средства защиты | Направление защиты | Ideco UTM |
|---|---|---|
| Межсетевой экран | Защита сетевой инфраструктуры | + |
| Средство обнаружения вторжений | Защита сетевой инфраструктуры | + |
| Средства защиты каналов передачи данных | Защита сетевой инфраструктуры | + |

| Реализация мер защиты ИСПДн (по 152-ФЗ от 27.07.2006) | |
|---|---|
| **Меры безопасности** | **Ideco UTM** |
| контроль доступа (включая фильтрацию и контроль соединений) к серверам ИСПДн, размещенным в помещениях, принадлежащих оператору; | + |
| контроль доступа (включая фильтрацию и контроль соединений) к серверам ИСПДн, размещенным в ЦОД; | + |
| контроль межсетевого доступа к серверам и другим компонентам ИСПДн (включая автоматизированные рабочие места пользователей, на которых осуществляется обработка персональных данных), размещенным в помещениях, принадлежащих оператору; | + |
| контроль доступа к ресурсам сети «Интернет»; | + |
| **Реализация мер защиты ИСПДн (по 152-ФЗ от 27.07.2006)** | |
| разграничение (контроль) доступа к категориям сетевых ресурсов, размещенным в ЦОД (web-серверы, базы данных, приложения и т.д.). | + |
| осуществление фильтрации сетевого трафика для отправителей информации, получателей информации и всех операций передачи контролируемой МЭ информации к узлам информационной системы и от них; | + |
| обеспечение фильтрации для всех операций перемещения через МЭ информации к узлам информационной системы и от них; | + |
| осуществление фильтрации, основанной на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия; | + |
| осуществление явного разрешения или запрета информационного потока, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации, основанном на идентифицированных атрибутах; | + |

| | |
|---|---|
| блокирование всех информационных потоков, проходящие через нефункционирующий или функционирующий некорректно МЭ; | + |
| осуществление регистрации и учета выполнения проверок информации сетевого трафика и предоставление указанной информации уполномоченным администраторам; | + |
| осуществление идентификации и аутентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора; | + |
| поддерживание определенных ролей по управлению МЭ; | + |
| обеспечение перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному функционированию. | + |