ГАЗИНФОРМ СЕРВИС

Программный комплекс по защите системно-технической инфраструктуры «Efros Defence Operations»

Описание применения

Санкт-Петербург, 2024

Аннотация

Данный документ представляет собой описание применения программного комплекса по защите системно-технической инфраструктуры «Efros Defence Operations» (ПК «Efros DO» или комплекс). Документ содержит сведения о назначении ПК «Efros DO», области его применения, применяемых методах, классе решаемых задач, ограничениях для применения, минимальной конфигурации технических средств.

Содержание

1 Назначение

1.1 Назначение программы

ПК «Efros DO» решает следующие задачи в области информационной безопасности (ИБ):

- контроль конфигураций и топологии сети;
- контроль целостности и проверки соответствия хостов и конечных точек;
- оптимизация и настройка межсетевых экранов (МЭ);
- анализ уязвимостей и построение векторов атак;
- сбор и отображение статистики по потокам данных в сети;
- централизованная сетевая идентификация администраторов и управление доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы TACACS+ и (или) RADIUS;
- автоматизация управления МЭ;
- защита DNS.

1.2 Структура ПК «Efros DO»

ПК «Efros DO» является высокопроизводительным комплексом по защите системно-технической инфраструктуры. Архитектура ПК «Efros DO» построена на основе микросервисов:

- платформа интеграции – единый интерактивный интерфейс, представляющий полный контроль над автоматизацией процессов ИБ;
- подсистема хранения данных;
- модуль обмена данными Apache Kafka;
- модуль хранения данных OpenSearch;
- модуль распределенного хранения объектов MinIO;
- функциональные модули – «Efros Network Assurance» («Efros NA»), «Efros Firewall Assurance» («Efros FA»), «Efros Network Access Control» («Efros NAC»), «Efros Integrity Check Compliance» («Efros ICC»), «Efros Vulnerability Control» («Efros VC»), «Efros Network Flow Analysis» («Efros «NFA»), «Efros Change Manager» («Efros CM»), «Efros Secure DNS» («Efros DNS»).
- микросервис лицензирования;
- микросервис аутентификации и авторизации;
- микросервис уведомлений и событий;

- микросервис объектов защиты;
- микросервис сбора метрик ИБ;
- микросервис маршрутизации запросов;
- микросервис генерации отчетов;
- микросервис базы знаний;
- микросервис драйверов сканера уязвимостей;
- микросервис системы заявок;
- микросервис отправки сообщений;
- микросервис расписаний;
- микросервис гостевых порталов;
- микросервис службы DNS;
- микросервис управления службами DNS;
- микросервис поддержки иерархии;
- микросервис управления агентами ПК «Efros DO»;
- микросервис поиска маршрутов для моделирования трафика на карте сети;
- микросервис управления контейнеризацией и кластеризацией.

Конфигурация ПК «Efros DO» зависит от наличия лицензий на функциональные модули: «Efros NA», «Efros FA», «Efros NAC», «Efros ICC», «Efros VC», «Efros NFA», «Efros CM», «Efros DNS».

1.3 Функциональные возможности программы

ПК «Efros DO» реализует следующие функциональные возможности:

- единая точка доступа (веб-интерфейс) к функциям комплекса и модулям интеграции;
- получение, обработка, интеграция и хранение данных, полученных из событий по объектам защиты (ОЗ) в ПК «Efros DO»;
- инвентаризация и ведение единого списка ОЗ;
- топология сети;
- мониторинг уведомлений о событиях контроля и об ошибках с ОЗ;
- мониторинг состояния ОЗ, подключенных к системе, в графическом и текстовом виде;
- формирование отчетов событий по ОЗ для модулей интеграции;

- ведение журнала системных событий;
- администрирование и настройка ПК «Efros DO»;
- идентификация и аутентификация администраторов комплекса на сервере ПК «Efros DO» с использованием идентификаторов и паролей;
- ведение списка администраторов комплекса с возможностью управления пользователями (добавление пользователей, групп пользователей, блокировка, активация, деактивация, удаление учетной записи пользователя, смена пароля пользователя);
- ролевое и дискреционное разграничение доступа пользователей комплекса к серверу ПК «Efros DO», к списку контролируемых на сервере ОЗ;
- передача событий безопасности для дальнейшей обработки (SIEM-системы);
- импорт сущностей из сторонних систем согласно заданному шаблону в формате .csv;
- интеграция со сканерами уязвимостей MaxPatrol 8, RedCheck и SafeERP Pentest;
- управление ролями пользователей комплекса;
- построение иерархии серверов;
- функции модуля контроля конфигураций и топологии сети «Efros NA»;
- функции модуля оптимизации и настройки МЭ «Efros FA»;
- функции модуля контроля целостности и проверки соответствия хостов и конечных точек «Efros ICC»;
- функции модуля анализа уязвимостей и построения векторов атак «Efros VC»;
- функции модуля сбора статистики по потокам данных в сети «Efros NFA»;
- функции модуля разграничения и контроля доступа в сети «Efros NAC»;
- функции модуля анализа и управления объектами защиты в разделе «Центр задач» «Efros CM»;
- функции модуля защиты DNS «Efros DNS».

Модули ПК «Efros DO» интегрируются в систему с учетом особенностей функционирования. Комплекс обеспечивает работу общих сервисов, техническое взаимодействие между ними и совместное функционирование процессов.

Единый веб-интерфейс ПК «Efros DO» позволяет пользователям с ролью администратора получить доступ к следующим возможностям:

1) Управление объектами сети (ОЗ, конечные точки, вектора атак):
   - просмотр ОЗ, клиентского оборудования (конечных точек сети);

- инвентаризация параметров сети и управление несконфигурированными ОЗ (добавление/удаление ОЗ);
- работа с базой знаний по ОЗ;
- ведение списка конечных точек сети;
- просмотр карты сети ОЗ;
- построение векторов атак;
- сканирование сети.

2) Контроль устройств:
   - настройка доступа к устройствам/группам устройств;
   - проверка безопасности;
   - проверка МЭ;
   - настройка профилей отчетов;
   - просмотр отчетов о событиях;
   - настройка обработчиков событий;
   - настройка профилей аутентификации;
   - настройка SNMP профилей;
   - настройка проверки доступности устройств.

3) Контроль доступа в сеть и к оборудованию:
   - управление активным сетевым оборудованием (АСО)/группами АСО;
   - управление сетевыми пользователями/группами сетевых пользователей, имеющих доступ к АСО;
   - настройка политик доступа;
   - настройка условий доступа;
   - настройка профилей оборудования;
   - настройка профилей авторизации;
   - загрузка ACL;
   - редактирование набора команд;
   - редактирование разрешенных протоколов аутентификации;
   - управление разрешенными MAC-адресами;
   - ведение словарей атрибутов;
   - создание и управление гостевыми порталами.

4) Управление агентами «Efros Defence Operations» (агент ПК «Efros DO» или агент):
   - учет установленных агентов на контролируемых конечных точках;
   - настройка политик безопасности и контроля целостности;
   - управление профилями настроек агентов;
   - работа с инсталляционными пакетами для установки и обновления агентов и дополнительных модулей.
5) Защита DNS:
   - управление черным и белым списками;
   - настройка правил IDS/IPS;
   - настройка защиты DNS-трафика;
   - настройка серверов пересылки.
6) Управление заявками в разделе «Центр задач».
7) Управление отчетами для ОЗ.
8) Просмотр и экспорт событий.
9) Администрирование:
   - управление пользователями/группами пользователей;
   - управление лицензиями на подключаемые модули;
   - ведение списка корневых, серверных и клиентских сертификатов, создание запросов на сертификаты;
   - настройка планировщика задач и событий.
10) Управление настройками:
   - настройка подключения к сервисам протоколов TACACS+ и RADIUS;
   - настройка источника данных (LDAP, Active Directory, профили сертификатов);
   - управление модулями встроенных и пользовательских типов устройств;
   - настройка сервера обновлений для базы уязвимостей;
   - управление хранением данных;
   - настройка почтовых серверов;
   - импорт данных;
   - настройка DNS-сервера для базы знаний;
   - настройка внешних систем (внешние серверы RADIUS, внешняя система аутентификации, SMS-провайдеры);

— построение иерархии серверов.

11) Мониторинг:

— визуализация процессов, обеспечивающих ИБ, с помощью встроенных и гибко настраиваемых схем в графическом виде с текстовым пояснением.

В ПК «Efros DO»:

1) Реализована поддержка протоколов TACACS+ и RADIUS для аутентификации, авторизации и учета действий пользователя на сетевых устройствах.
2) Установлены внешние модули, отвечающие за активный аудит сетевого оборудования, серверных и клиентских операционных систем (ОС):

— модуль взаимодействия с сетевыми устройствами (использует протоколы SSH/Telnet);

— модуль управления устройствами, модуль взаимодействия с устройствами Континент, Dionis, Docker (использует протоколы SCP, SFTP);

— модуль взаимодействия с CheckPoint (использует протоколы CPMI и LEA);

— модуль отправки писем по протоколу SMTP (использует протокол SMTP);

— модуль syslog-сервера и отправки syslog-сообщений (использует протокол Syslog);

— модуль отправки сообщений через MS Exchange (использует Microsoft Exchange Web Services Managed API);

— сканер сети для последующего добавления найденных устройств в список устройств (использует протокол SNMP);

— модуль взаимодействия с MS SQL (использует протокол Microsoft TDS);

— модуль взаимодействия с Oracle (использует протокол Oracle .Net);

— модуль взаимодействия с PostgreSQL, Jatoba (использует протокол PostgreSQL Protocol);

— модуль взаимодействия с MySQL (использует протокол MySQL);

— модуль взаимодействия с Firebird (использует протокол Firebird Wire Protocol);

— модуль взаимодействия с UserGate (использует протокол XML-RPC);

— windows-агент (использует проприетарный протокол на базе HTTPS);

— модуль взаимодействия с устройствами по протоколу REST;

— модуль взаимодействия со службами DNS по протоколу DNS.

3) Созданы правила доступа путем сопоставления пользователя и сетевого устройства, и назначения пользователю списка доступных команд. Обновления в

настройках доступа применяются сразу после изменения параметров пользователя/групп пользователей и устройства/групп устройств.

ПК «Efros DO» обеспечивает анализ правил МЭ, активный контроль сетевого оборудования, серверных и клиентских ОС, автоматизированных систем управления технологическим процессом (АСУ ТП), виртуальных сред производства компаний:

- Cisco Systems, Inc. (ACS, ACI, ASA, AsyncOS, CatOS, FTD, FWSM Module, IOS, IOS XE, IOS XR, IPS, NX-OS, PIX, SMB, WAP, WLC, FMC 6.x (с поддержкой MDS), Firepower);
- 3Com Corporation (3ComOS);
- ЗАО «Российская корпорация средств связи» (RSOS9000, RS7750, RSOA700, Onyx);
- С-Терра СиЭсПи (NME-RVPN, VPN Gate);
- HP, Inc. (BladeSystem, Comware Switch, Procurve, Virtual Connect, UX, Aruba);
- Allied Telesis (Allied-Telesis AT-GS950);
- Lenovo (ENOS 8.4, Cumulus, FabricOS);
- КриптоПро (NGate);
- Blue Coat Systems, Inc., ранее Crossbeam Systems, Inc. (XOS v.9);
- Oracle Corporation (системы управления базами данных (СУБД) Oracle 10g, SunOS, СУБД MySQL);
- D-Link Corporation (DES, DGS, DGS 3130/3630);
- ООО «СайберЛимфа» (DATAPK);
- RAISECOM Technology (ISCOM);
- Korenix Technology Co., Ltd (JetNet);
- Kubernetes;
- ZyXEL Communications Corp. (ZyNOS);
- Zelax (Zelax M-1 Mera, Zelax ZES);
- Edge-core (ECS);
- ExtremeNetworks (Extreme 220 series, ExtremeXOS);
- Check Point Software Technologies, Inc. (R80 Management Server, SecurePlatform, GAiA, SmartCenter, GAiA Embedded, Domain Management Server, Maestro Orchestrator);
- ООО «Кьютек» (QSW);
- MikroTik (Mikrotik RouterOS);

- Moxa, Inc (EDS, MGate, NPort 5100 Series);
- Huawei Technologies Co., Ltd (Quidway);
- ОАО «ИнфоТеКС» (VipNet Coordinator, VipNet xFirewall);
- НПП «Фактор-ТС» (Dionis NX версии 1.1, 1.2 и 2.0);
- Juniper Networks, Inc (JUNOS);
- ООО «Предприятие «Элтекс» (Eltex MES, ESR, WLC, ME, MES24xx, WOP/WEP);
- ООО «Бифорком Тек» (коммутаторы серии CS2100);
- ООО «Код Безопасности» (Континент);
- ООО «ТИОНИКС» (TIONIX);
- Palo Alto Networks, Inc (PanOS);
- ОАО НПП «Полигон» (Арлан, ИнЗер);
- UiPath Inc (Uipath Studio, Uipath Orchestrator, Uipath Robot);
- WatchGuard Technologies, Inc. (WatchGuard Fireware OS, WatchGuard Fireware XTM OS);
- Rockwell Automation, Inc (Rockwell Cisco IOS);
- TFortis (PSW); Siemens AG (Siemens Scalance X-300, X-400 series, Simatic WinCC);
- ОС Unix/Linux (AIX, Oracle SunOS, HP-UX, AltLinux, Red Hat, Debian, Manjaro, Ubuntu, Mint, Fedora, FreeBSD, Red OS, Astra Linux);
- ОС Microsoft Windows (XP, vista, 7, 8, 10, 2000, 2003, 2008r2, 2012, 2012r2, 2016, 2019);
- ООО «Базальт СПО» (Альт Сервер Виртуализации 9.2 в PVE исполнении (PVE версия 6.3));
- Microsoft Corporation (Microsoft SQL Server 2000, 2005, 2008, 2012, 2016);
- СУБД PostgreSQL;
- ООО «Газинформсервис» (СУБД «Jatoba»);
- Firebird Foundation (СУБД Firebird);
- Docker;
- Open Virtualization Alliance (KVM);
- Инфолэнд (zVirt);
- НАТЕКС (NetXpert);

- NSGate (NIS);
- Hirschmann (MAR);
- UserGate (UserGate UTM);
- AVAYA;
- Azimut (Marlin);
- AdAstrA Research Group, Ltd (SCADA TRACE MODE);
- Fortinet (Fortinet FortiGate, Fortinet FortiGate VDOM, Fortinet FortiWLC, Fortinet FortiSwitch);
- НПФ «Система-Сервис» (Аргус);
- АО «ЭлеСи» (SCADA Infinity);
- АО «ТРЭИ» (ПЛК Trei);
- АО «ЭЗАН» (ПЛК Ezan);
- АО «Атомик Софт» (SCADA Alpha.HMI);
- ООО «ИнСАТ» (MasterSCADA);
- ООО «Прософт-Системы» (ПЛК Regul);
- ООО «ФАСТВЕЛ ГРУПП» (ПЛК Fastwel);
- GE Digital (CIMPLICITY, iFix, GENESIS32);
- Schneider Electric (Vijeo Citect SCADA);
- Compressor Controls Corporation (CCC) (TrainTools, TrainView);
- ООО «Газприборавтоматика» (Zond2006, Zond2015);
- Emerson (SCADA DeltaV);
- Yokogawa Electric Corporation (CENTUM VP);
- НПО «Текон-Автоматика» (SCADA АСУД-248);
- ООО «НПА Вира Реалтайм» (ПК «Сириус-ИС»);
- Rubytech (СКАЛА-Р 1.91);
- Verano (RTAP A.08.10 (Windows), RTAP A.09.00 (Linux));
- Wonderware InTouch (7, 8, 10, 11);
- SNR.SYSTEMS (SNR);
- Weidmüller Interface GmbH & Co. KG (Weidmüller).

Оборудование, поддерживаемое серверной частью ПК «Efros DO» в зависимости от установленной лицензии, приведено в Приложении А.

1.3.1 Модуль контроля конфигураций и топологии сети «Efros Network Assurance»

Модуль «Efros NA» реализует следующие функциональные возможности ПК «Efros DO»:

- контроль изменения конфигураций сетевого оборудования;
- контроль изменения конфигураций МЭ;
- проверки соответствия безопасности сетевого оборудования;
- проверки соответствия безопасности МЭ;
- моделирование трафика на основе маршрутов и правил МЭ.

Данные возможности доступны только при наличии лицензии на использование модуля «Efros NA».

1.3.2 Модуль оптимизации и настройки межсетевых экранов «Efros Firewall Assurance»

Модуль «Efros FA» реализует следующие функциональные возможности ПК «Efros DO»:

- формирование отчетов по оптимизации правил, выявление теневых, избыточных, неиспользуемых правил;
- проверка правил МЭ на соответствие требованиям запрета или разрешения транзитного трафика между зонами;
- проверка правил МЭ на соответствие требованиям настройки;
- зонный анализ;
- формирование стандартов МЭ.

Данные возможности доступны только при наличии лицензии на использование модуля «Efros FA».

1.3.3 Модуль контроля целостности и проверки соответствия хостов и конечных точек «Efros Integrity Check Compliance»

Модуль «Efros ICC» реализует следующие функциональные возможности ПК «Efros DO»:

- контроль изменения конфигураций ОС, виртуализации, контейнеров и прикладного программного обеспечения (ППО);
- контроль целостности файлов ОС, виртуализации, контейнеров и ППО;

— проверки соответствия безопасности ОС, виртуализации, контейнеров и ППО.

Данные возможности доступны только при наличии лицензии на использование модуля «Efros ICC».

1.3.4 Модуль анализа уязвимостей и построения векторов атак «Efros Vulnerability Control»

Модуль «Efros VC» реализует следующие функциональные возможности ПК «Efros DO»:

— выявление известных уязвимостей на основе версии ОС;

— синхронизация списков уязвимостей с собственной базой данных по уязвимостям (БДУ);

— синхронизация с активными сканерами уязвимостей для получения информации об ОЗ;

— построение векторов атак.

Данные возможности доступны только при наличии лицензии на использование модуля «Efros VC».

1.3.5 Модуль сбора статистики по потокам данных в сети «Efros Netflow Analyzer»

Модуль «Efros NFA» реализует следующие функциональные возможности ПК «Efros DO»:

— предоставление информации по соединениям с параметрами скорости, длительности и принадлежности к адресам;

— сбор статистики использования сетевого трафика по соединениям и анализ активности;

— контроль изменений IP и MAC-адресов;

— работа с протоколами NetFlow, sFlow, IPFIX и NetStream.

Данные возможности доступны только при наличии лицензии на использование модуля «Efros NFA».

1.3.6 Модуль разграничения и контроля доступа в сети «Efros Network Access Control»

Модуль «Efros NAC» реализует следующие функциональные возможности ПК «Efros DO»:

- управление доступом в сетевые сегменты с применением расширенных политик доступа в сеть, управление административным доступом к АСО;
- формирование расширенных политик управления доступом на основе собранной статистики и создание набора политик;
- профилирование конечных устройств (конечных точек);
- создание новых правил авторизации на основе уже существующих;
- регистрация и учет попыток подключения конечных точек и пользователей;
- синхронизация пользователей с источником LDAP;
- взаимодействие со службами каталогов LDAP (MS Active Directory, FreeIPA, OpenLDAP, ALD Pro);
- трассировка сессий RADIUS аутентификации;
- проверка значений RADIUS атрибутов на основе регулярных выражений;
- отправка уведомлений в RADIUS о событиях на конечных точках (CoA, Disconnect);
- загрузка RADIUS атрибутов производителей;
- использование политик TACACS+ для доступа на сетевое оборудование;
- трассировка сессий TACACS+ аутентификации;
- доступ на оборудование по протоколу TACACS+;
- гостевой портал;
- передача событий безопасности для дальнейшей обработки (SIEM-системы);
- интеграция с системой Cisco ACS\ISE (импорт пользователей АСО и списка сетевых устройств/конечных точек).

Данные возможности доступны только при наличии лицензии на использование модуля «Efros NAC».

1.3.7 Модуль анализа и управления объектами защиты в разделе «Центр задач» «Efros Change Manager»

Модуль «Efros CM» реализует возможность автоматизации управления жизненным циклом правил МЭ в разделе «Центр задач» ПК «Efros DO».

1.3.8 Модуль защиты DNS «Efros Secure DNS»

Модуль «Efros DNS» реализует следующие функциональные возможности ПК «Efros DO»:

- блокировка доступа к нежелательным сайтам;
- обнаружение и предотвращение атак на DNS-трафик.

1.4 Роли пользователей

Пользователями ПК «Efros DO» являются:

- пользователи (администраторы) ПК «Efros DO»;
- пользователи (администраторы) ОЗ;
- пользователи сервисов (сетевые пользователи), предоставляемых ОЗ (контролируемыми устройствами) и гостевыми порталами.

Возможности пользователя в ПК «Efros DO» зависят от назначенной роли и определяются настройкой прав и привилегий. Для пользователя сервисов определяется список доступных ОЗ и права доступа на них.

Пользователи сервисов не имеют доступа к веб-приложению ПК «Efros DO», но имеют доступ к назначенным в комплексе сетевым устройствам или ресурсам.

Каждой роли соответствует определенный набор прав и привилегий (таблица 1). Права доступа задаются при создании нового пользователя и по необходимости могут быть изменены пользователем с соответствующими привилегиями.

Таблица 1 – Привилегии и права, назначаемые пользователям ПК «Efros DO»

Группа привилегий	Привилегия	Права	Описание
Основные	Основные функции*	Управление	Доступ к разделам: — Мониторинг; — Объекты сети; — Отчеты (личные); — Центр задач (заявки, по которым является автором или участником). Возможность создания / редактирования / удаления ОЗ без права создания / редактирования возможностей (Контроль доступа, контроль устройств, потоки данных)
	Карта сети	Управление	Доступ к разделу: — Объекты сети/ Карта сети
	База знаний	Просмотр/ Управление	Доступ к разделу: — Объекты сети/ База знаний

Группа привилегий	Привилегия	Права	Описание
	Векторы атак	Просмотр/ Управление	Доступ к разделу: — Объекты сети/ Векторы атак
	Конечные точки	Просмотр/ Управление	Доступ к разделу: — Объекты сети/ Конечные точки
	Агенты	Просмотр/ Управление	Доступ к разделу: — Объекты сети/ Агенты
	Контроль устройств	Просмотр/ Управление	Доступ к разделу: — Контроль устройств. Доступ к возможности «Контроль устройств»
	Контроль доступа	Просмотр/ Управление	Доступ к разделу: — Контроль доступа; Доступ к возможности «Контроль доступа»
	Контроль доступа / Разрешенные MAC-адреса	Просмотр/ Управление	Доступ к разделу: — Контроль доступа/ Разрешенные MAC-адреса
	Контроль трафика	Просмотр/ Управление	Доступ к возможности «Контроль трафика»
	Гостевые порталы	Просмотр/ Управление	Доступ к гостевым порталам
	Отчеты / Общие	Просмотр/ Управление	— Просмотр – формирование отчета по шаблону, добавление шаблона в раздел «Личные». Удаление /изменение отчетов запрещено; — Управление – разрешены любые действия с шаблоном
	Центр задач / Администрирование	Просмотр/ Управление	Доступ к разделу: — Центр задач
	Защита DNS	Просмотр/ Управление	Доступ к разделу: — Защита DNS
	Журналы событий системы	Просмотр	Доступ к разделу: — События
Администрирование	Пользователи / Пользователи	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Пользователи. Вкладка «Пользователи»
	Пользователи / Роли	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Роли. Вкладка «Роли»
	Пользователи / Настройки безопасности	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Пользователи. Вкладка «Настройки безопасности»

Группа привилегий	Привилегия	Права	Описание
	Пользователи / Active Directory	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Пользователи. Вкладка «Active Directory»
	Лицензия	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Лицензии
	Сертификаты	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Сертификаты
	Планировщик	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Планировщик
Настройки	Контроль доступа	Просмотр/ Управление	Доступ к разделу: — Настройки/ Группа «Контроль доступа»
	Контроль устройств	Просмотр/ Управление	Доступ к разделу: — Настройки/ Группа «Контроль устройств»
	Общие	Просмотр/ Управление	Доступ к разделу: — Настройки/ Группа «Общие» (кроме «Импорт данных» и «Агенты)
	Общие / Импорт данных	Управление	Доступ к разделу: — Настройки/ Группа «Общие»/ Импорт данных
	Общие / Агенты	Просмотр/ Управление	Доступ к разделу: — Настройки/ Группа «Общие»/ Агенты
	Общие / Иерархия серверов	Просмотр/ Управление	Доступ к разделу: — Настройки/ Группа «Общие»/ Иерархия серверов

Примечания:

1) Значение «Просмотр» в столбце «Права» – чтение конфигураций, состояний ОЗ;

2) Значение «Управление» в столбце «Права» – просмотр, редактирование конфигураций, изменение прав пользователей;

3) Значение «Просмотр/Управление» в столбце «Права» – возможность выбора одного из вариантов прав пользователей;

* – Привилегия «Основные функции» активна по умолчанию, выключить данную привилегию невозможно

После установки и настройки ПК «Efros DO» в базе данных автоматически создается учетная запись пользователя с ролью встроенного системного администратора «GlobalAdministrator».

2 Условия применения

Минимальный состав технических средств электронно-вычислительной машины (ЭВМ)[1] для установки серверной части и внешних модулей ПК «Efros DO» рассчитывается на основе данных, приведенных в таблице 2.

Таблица 2 – Технические требования к среде функционирования ПК «Efros DO» и ППО

Элемент	Параметр		
Количество ОЗ	До 500	До 1000	До 2000*
Требования к программному обеспечению			
ОС	Astra Linux Special Edition (v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.), поддерживается установка на ОС с ядром 5.15-Generic; Альт Server 10; РЕД ОС (v. 7.3), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
СУБД	СУБД PostgreSQL 13; СУБД «Jatoba» (поддерживается версия «ядра» 4)		
Прикладное ПО	Docker v. 18.03.0 и выше; Docker-compose v. 2.9.0; Confluent Kafka v. 5.5.0 СУБД OpenSearch v. 1.3.7; СУБД MinIO v. 220218		
Требования к аппаратному обеспечению			
Процессор	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память	от 32 Гб	от 48 Гб	от 64 Гб
Жесткий диск (комплекс + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер комплекса	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД	от 400 Гб	от 1000 Гб	от 2200 Гб
Сетевая карта	1 Гбит/с	1 Гбит/с	1 Гбит/с
Требования для функционирования модуля «Efros NAC»			
TACACS+	порт 49		
RADIUS	порты 1812, 1813		
Гостевые порталы	порт 5802		
Требования для функционирования модуля «Efros NFA»			
Netflow v9+, IPFIX	порт 2056		
sFlow	порт 6343		
Netflow v5	порт 2055		
Требования для функционирования модуля «Efros DNS»			
DNS	Порт 53		
Требования для функционирования модулей «Efros NA», «Efros FA»,			

[1] Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86 (x86_64)

Элемент	Параметр
«Efros ICC», «Efros VC», «Efros CM»	
Для подключения Windows-агента	порт 20002
syslog	порт 514
SNMP Trap / Inform	порт 162
Windows-агент	
ОС	Windows**
Процессор	1,6 ГГц
Оперативная память	1 Гб
Жесткий диск	100 Мб
Агент «Efros DO»	
ОС	Windows** (поддерживается только 64-разрядная версия ОС); РЕД ОС (рабочая станция, сервер) (7.3 и выше); Astra Linux Special Edition (1.6 и выше); Ubuntu (22.04 и выше); MacOS Monterey (12.6 и выше) x86_64
Суппликант ПК «Efros DO»	
ОС	Windows** (поддерживается только 64-разрядная версия ОС); РЕД ОС (рабочая станция, сервер) (7.3 и выше); Astra Linux Special Edition (1.6 и выше)
Минимальные требования к производительности рабочей станции, на которую устанавливается агент ПК «Efros DO» и суппликант ПК «Efros DO», обусловлены требованиями используемой ОС	
Единый интерактивный веб-интерфейс – обеспечивает доступ пользователей к функциональности ПК «Efros DO» с использованием браузера, который работает на основе проекта с открытым кодом Chromium	
*От 2000 ОЗ – параметры рассчитываются индивидуально. Обратитесь в техподдержку **ОС серии Windows: — Windows Server 2008R2 Foundation Edition SP1 (64-разрядная); — Windows Server 2008R2 Standard Edition SP1 (64-разрядная); — Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная); — Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная); — Windows Server 2012/2012R2 Foundation (64-разрядная); — Windows Server 2012/2012R2 Essentials (64-разрядная); — Windows Server 2012/2012R2 Standard (64-разрядная); — Windows Server 2012/2012R2 Datacenter (64-разрядная); — Windows Server 2016 Standard (64-разрядная); — Windows Server 2016 Datacenter (64-разрядная); — Windows Server 2016 Essentials (64-разрядная); — Windows Server 2019 Standard (64-разрядная); — Windows Server 2019 Datacenter (64-разрядная); — Windows Server 2019 Essentials (64-разрядная); — Windows 7 Professional SP1 (32-разрядная/64-разрядная); — Windows 7 Enterprise SP1 (32-разрядная/64-разрядная);	

Элемент	Параметр
— Windows 7 Ultimate SP1 (32-разрядная/64-разрядная); — Windows 8.1 Core (32-разрядная/64-разрядная); — Windows 8.1 Professional (32-разрядная/64-разрядная); — Windows 8.1 Enterprise (32-разрядная/64-разрядная); — Windows 10 Home (32-разрядная/64-разрядная); — Windows 10 Pro (32-разрядная/64-разрядная); — Windows 10 Enterprise (32-разрядная/64-разрядная); — Windows 11 Home (64-разрядная); — Windows 11 Pro (64-разрядная); — Windows 11 Enterprise (64-разрядная)	

Для эксплуатации и эффективного применения ПК «Efros DO» необходимо использование на ЭВМ лицензионного системного программного обеспечения.

3 Задачи

ПК «Efros DO» решает следующие задачи:

- контроль конфигураций и топологии сети (модуль «Efros NA»);
- оптимизация и настройка МЭ (модуль «Efros FA»);
- централизованная сетевая идентификация администраторов и управление доступом на сетевых устройствах, у которых на клиентском уровне поддерживаются протоколы TACACS+ и (или) RADIUS (модуль «Efros NAC»);
- контроль целостности и проверки соответствия хостов и конечных точек (модуль «Efros ICC»);
- анализ уязвимостей и построение векторов атак (модуль «Efros VC»);
- сбор и отображение статистики по потокам данных в сети (модуль «Efros NFA»);
- автоматизация управления МЭ (модуль «Efros CM»)
- защита DNS (модуль «Efros DNS»).

Подробное описание работы модулей содержится в документе «Руководство пользователя ПК «Efros DO».

3.1 Возможности карты сети

В ПК «Efros DO» для контроля конфигураций и топологии сети реализована возможность формирования карты сети.

В таблице 3 приведен перечень типов устройств с указанием поддерживаемых возможностей формирования карты сети.

Таблица 3 – Возможности формирования карты сети

Тип устройства	Интерфейсы	Sub интерфейсы	Маршруты	PBR	Натирование (NAT)	Туннели IPSec/IPIir	Туннели GRE	Правила МЭ	Implicit rule
Сетевые устройства									
3Com OS	нет	нет	нет	-	нет	нет	-	нет	нет
Allied-Telesis AT-GS950	нет	нет	нет	-	нет	нет	-	нет	нет
Avaya	нет	нет	нет	-	нет	нет	-	нет	нет
Check Point GAiA	да	да	нет	-	нет	нет	-	да	нет
Check Point GAiA с контролем файлов по SSH	да	да	да	да	нет	да	-	да	да
Check Point GAiA Embedded	да	да	нет	-	нет	нет	-	да	нет
Check Point GAiA Embedded с контролем файлов по SSH	да	да	да	да	нет	да	-	да	да
Check Point SmartCenter	нет	нет	-	-	-	-	-	нет	нет
Check Point R80 Management Server	нет	нет	-	-	-	-	-	нет	нет
Check Point Domain Management Server	нет	нет	-	-	-	-	-	нет	нет
Check Point Gateway	нет	нет	нет	-	нет	да	-	да	да
Check Point SecurePlatform	нет	нет	нет	-	нет	нет	-	нет	нет
Check Point Maestro Orchestrator	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco ACI	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco ACS	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco ASA	да	нет	да	-	нет	да	-	да	да
Cisco ASA Context	да	нет	да	-	нет	да	-	да	да
Cisco ASA Context (Auto)	да	нет	да	-	нет	да	-	да	да
Cisco IronportAsyncOS	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco CatOS	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco Firepower Device	да	нет	нет	-	нет	нет	-	да	да
Cisco FTD	нет	нет	да	-	нет	нет	-	нет	нет
Cisco FTD с контролем файлов по SSH	да	нет	да	-	нет	нет	-	да	да
Cisco FWSM Module	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco IOS	да	да	да	да	да	нет	-	да	да
Cisco IOS XE	нет	нет	нет	-	нет	нет	-	да	нет

Тип устройства	Интерфейсы	Sub интерфейсы	Маршруты	PBR	Натирование (NAT)	Туннели IPSec/IPIir	Туннели GRE	Правила МЭ	Implicit rule
Cisco IOS XR	да	нет	да	-	нет	нет	-	да	нет
Cisco IPS	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco NX-OS	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco PIX	нет	нет	да	-	да	да	-	да	нет
Cisco SMB	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco WAP	нет	нет	нет	-	нет	нет	-	нет	нет
Cisco WLC	нет	нет	нет	-	нет	нет	-	нет	нет
Crossbeam XOS v.9	нет	нет	нет	-	нет	нет	-	нет	нет
Phoenix contact	да	нет	нет	-	нет	нет	-	нет	нет
H3C	да	да	да	-	нет	нет	-	да	нет
Dionis-LX	нет	нет	нет	-	нет	нет	-	нет	нет
Dionis-NX 1.1	да	да	нет	-	нет	да	-	да	нет
Dionis-NX 1.2	да	да	нет	-	нет	да	-	да	нет
Dionis-NX 2.0	да	да	да	-	да	да	-	да	да
Файл конфигурации Dionis-LX	нет	нет	нет	-	нет	нет	-	нет	нет
Файл конфигурации Dionis-NX	да	да	да	-	да	да	-	да	да
D-Link DES	нет	нет	нет	-	нет	нет	-	нет	нет
D-Link DGS	нет	нет	нет	-	нет	нет	-	нет	нет
D-Link DGS 1210	нет	нет	нет	-	нет	нет	-	нет	нет
D-Link DGS 3130/3630	нет	нет	нет	-	нет	нет	-	нет	нет
Edge-Core ECS	нет	нет	нет	-	нет	нет	-	нет	нет
Eltex ESR	да	да	да	-	да	да	-	да	да
Eltex ME	нет	нет	нет	-	нет	нет	-	нет	нет
Eltex MES	да	да	да	-	нет	нет	-	да	да
Eltex MES 24xx	да	нет	да	-	нет	нет	-	нет	нет
Eltex WLC	да	да	да	-	да	да	-	да	нет
Eltex WOP/WEP	нет	нет	нет	-	нет	нет	-	нет	нет
Extreme 220 series	нет	нет	нет	-	нет	нет	-	нет	нет
ExtremeXOS	да	нет	да	-	нет	нет	-	нет	нет
Fortinet FortiGate	да	да	нет	-	нет	нет	-	да	да
Fortinet FortiGate VDOM	нет	нет	нет	-	нет	нет	-	нет	нет
Fortinet FortiGate VDOM (auto)	да	да	нет	-	нет	нет	-	да	да

Тип устройства	Интерфейсы	Sub интерфейсы	Маршруты	PBR	Натирование (NAT)	Туннели IPSec/IPIir	Туннели GRE	Правила МЭ	Implicit rule
Fortinet FortiSwitch	нет	нет	нет	-	нет	нет	-	нет	нет
Fortinet FortiWLC	нет	нет	нет	-	нет	нет	-	нет	нет
Hirschmann MAR	нет	нет	нет	-	нет	нет	-	нет	нет
HP Aruba	нет	нет	нет	-	нет	нет	-	нет	нет
HP BladeSystem	нет	нет	нет	-	нет	нет	-	нет	нет
HP Comware Switch	нет	нет	нет	-	нет	нет	-	нет	нет
HP Procurve	нет	нет	нет	-	нет	нет	-	нет	нет
HP Virtual Connect	нет	нет	нет	-	нет	нет	-	нет	нет
Huawei VRP	да	нет	да	-	нет	нет	-	да	да
Juniper JunOS	нет	нет	нет	-	нет	нет	-	нет	нет
Korenix JetNet	нет	нет	нет	-	нет	нет	-	нет	нет
Lenovo Cumulus	нет	нет	нет	-	нет	нет	-	нет	нет
Lenovo ENOS 8.4	нет	нет	нет	-	нет	нет	-	нет	нет
Lenovo FabricOS 8.x	нет	нет	нет	-	нет	нет	-	нет	нет
Marlin	да	нет	да	-	нет	нет	-	да	да
Mikrotik RouterOS	нет	нет	нет	-	нет	нет	-	нет	нет
Moxa EDS	нет	нет	нет	-	нет	нет	-	нет	нет
Moxa MGate	нет	нет	нет	-	нет	нет	-	нет	нет
Moxa Nport 5150	нет	нет	нет	-	нет	нет	-	нет	нет
Nateks NX-3400	нет	нет	нет	-	нет	нет	-	нет	нет
Nateks NX-5100	нет	нет	нет	-	нет	нет	-	нет	нет
Nateks NXI-3030	нет	нет	нет	-	нет	нет	-	нет	нет
Nateks NXI-3050	нет	нет	нет	-	нет	нет	-	нет	нет
КриптоПро TLS шлюз	нет	нет	нет	-	нет	нет	-	нет	нет
NS Gate NIS	нет	нет	нет	-	нет	нет	-	нет	нет
Palo Alto Pan-OS 7	нет	нет	нет	-	нет	нет	-	нет	нет
Palo Alto Pan-OS 9	нет	нет	нет	-	нет	нет	-	нет	нет
PKCC OmniAccess 700	нет	нет	нет	-	нет	нет	-	нет	нет
PKCC OmniSwitch 6850	нет	нет	нет	-	нет	нет	-	нет	нет
PKCC OmniSwitch 7710	нет	нет	нет	-	нет	нет	-	нет	нет
PKCC OmniSwitch 7750	нет	нет	нет	-	нет	нет	-	нет	нет
PKCC OmniSwitch 9000	нет	нет	нет	-	нет	нет	-	нет	нет

Тип устройства	Интерфейсы	Sub интерфейсы	Маршруты	PBR	Натирование (NAT)	Туннели IPSec/IPIir	Туннели GRE	Правила МЭ	Implicit rule
РКСС Onyx	нет	нет	нет	-	нет	нет	-	нет	нет
QTech QSW	нет	нет	нет	-	нет	нет	-	нет	нет
Raisecom ISCOM	нет	нет	нет	-	нет	нет	-	нет	нет
Rockwell Cisco IOS	нет	нет	нет	-	нет	нет	-	нет	нет
Tfortis PSW	нет	нет	нет	-	нет	нет	-	нет	нет
Siemens Scalance X-300 series	нет	нет	нет	-	нет	нет	-	нет	нет
Siemens Scalance X-400 series	нет	нет	нет	-	нет	нет	-	нет	нет
S-Terra VPN Gate	да	нет	да	-	нет	да	-	да	да
SNR	да	нет	да	-	нет	нет	-	да	нет
UserGate UTM 5	да	нет	да	-	нет	нет	-	да	нет
UserGate UTM 6	да	нет	да	-	да	да	-	да	да
UserGate UTM 7	да	нет	да	-	да	да	-	да	да
VipNet Coordinator HW	да	нет	да	-	да	да	-	да	да
VipNet xFirewall	да	нет	да	-	да	нет	-	да	да
VipNet Prime	нет	нет	нет	-	нет	нет	-	нет	нет
Weidmuller	нет	нет	нет	-	нет	нет	-	нет	нет
WatchGuard Fireware OS	нет	нет	нет	-	нет	нет	-	нет	нет
WatchGuard Fireware XTM OS	нет	нет	нет	-	нет	нет	-	нет	нет
Zelax M-1-MEGA	нет	нет	нет	-	нет	нет	-	нет	нет
Zelax ZES	нет	нет	нет	-	нет	нет	-	нет	нет
ZyXEL ZyNOS	нет	нет	нет	-	нет	нет	-	нет	нет
Континент Криптошлюз	да	нет	да	-	да	нет	-	да	нет
Континент Криптокоммутатор	да	нет	да	-	нет	нет	-	да	нет
Континент Детектор атак	да	нет	да	-	нет	нет	-	да	нет
Континент v.4 Узел безопасности	да	нет	да	-	нет	нет	-	да	нет
Континент v.4 Узел безопасности с ЦУС	да	нет	да	-	нет	нет	-	да	нет
Бифорком, коммутаторы серии CS2100	да	нет	да	-	нет	нет	-	да	нет
Полигон Арлан	нет	нет	нет	-	нет	нет	-	нет	нет
Полигон ИнЗер	нет	нет	нет	-	нет	нет	-	нет	нет
Операционные системы									

Тип устройства	Интерфейсы	Sub интерфейсы	Маршруты	PBR	Натирование (NAT)	Туннели IPSec/IPIir	Туннели GRE	Правила МЭ	Implicit rule
Windows	да	нет	нет	-	-	-	-	нет	нет
Linux	да	нет	да	-	-	да	-	да	нет
AIX	да	нет	да	-	-	нет	-	да	нет
HP-UX	да	нет	да	-	-	нет	-	да	нет
Alt Linux	да	нет	да	-	-	нет	-	да	нет
Astra Linux	да	нет	да	-	-	да	-	да	нет
Debian	да	нет	да	-	-	да	-	да	нет
FreeBSD	да	нет	да	-	-	нет	-	да	нет
Red OS	да	нет	да	-	-	да	-	да	нет
SunOS	да	нет	да	-	-	нет	-	да	нет
Примечания: «да» – реализовано; «нет» – не реализовано; «-» – не поддерживается устройством									

3.2 Универсальный отчет правил межсетевых экранов

В ПК «Efros DO» для МЭ реализована возможность формирования универсального отчета «Правила МЭ». Данный отчет содержит информацию об установленных на МЭ различных типов правил в удобном для пользователя виде. Отчет для различных типов МЭ выводится в едином стиле.

В таблице 4 приведен перечень типов МЭ с указанием поддерживаемых возможностей отчета «Правила МЭ». В таблице 5 приведен перечень типов МЭ с указанием поддерживаемых дополнительных данных отчета «Правила МЭ».

Таблица 4 – Возможности отчета «Правила МЭ»

Тип МЭ	Number	Name	Action	Protocol	Source	Source Port	Destination	Destination Port	Service	Description (remark)	Hit Count	Status (enable/disable)	UUID	Additional
Cisco ASA	да	нет	да	да	да	да	да	да	-	да	да	да	-	да
Cisco ASA Context	да	нет	да	да	да	да	да	да	-	да	да	да	-	да
Cisco PIX	нет	нет	да	да	да	да	да	да	-	да	нет	да	-	да

Тип МЭ	Number	Name	Action	Protocol	Source	Source Port	Destination	Destination Port	Service	Description (remark)	Hit Count	Status (enable/disable)	UUID	Additional
Cisco Firepower Device	да	да	да	-	да	да	да	да	-	да	да	да	-	да
Cisco FTD с контролем файлов по SSH	да	да	да	-	да	да	да	да	-	да	да	да	-	да
Cisco IOS	да	нет	да	да	да	да	да	да	-	да	да	да	-	да
Cisco IOS XE	да	нет	да	да	да	да	да	да	-	да	да	нет	-	да
Cisco IOS XR	нет	нет	да	да	да	да	да	да	-	да	да	нет	-	да
Check Point Gateway	да	да	да	-	да	-	да	-	да	да	да	да	да	да
Check Point GAiA с контролем файлов по SSH	да	да	да	-	да	-	да	-	да	да	да	да	-	да
Check Point GAiA Embedded с контролем файлов по SSH	да	да	да	-	да	-	да	-	да	да	да	да	-	да
H3C	да	да	да	да	да	да	да	да	-	да	нет	нет	-	да
Huawei VRP	да	нет	да	да	да	да	да	да	-	-	нет	да	-	да
Eltex MES	да	нет	да	да	да	да	да	да	нет	нет	да	да	-	да
Eltex ESR	да	нет	да	да	да	да	да	да	нет	нет	нет	да	-	да
Eltex WLC	да	нет	да	да	да	да	да	да	нет	нет	нет	да	-	да
Dionis NX 1.1	да	нет	да	да	да	да	да	да	нет	да	да	да	-	да
Dionis NX 1.2	да	нет	да	да	да	да	да	да	нет	да	да	да	-	да
Dionis-NX 2.0	да	нет	да	да	да	да	да	да	нет	да	да	да	-	да
Файл конфигурации Dionis-NX	да	нет	да	да	да	да	да	да	нет	да	нет	да	-	да
Fortinet FortiGate	да	да	да	-	да	-	да	-	да	да	да	да	-	да
Fortinet FortiGate VDOM (auto)	да	да	да	-	да	-	да	-	да	да	да	да	-	да
UserGate UTM 5	да	да	да	-	да	-	да	-	да	нет	нет	да	-	да
UserGate UTM 6	да	да	да	-	да	-	да	-	да	нет	нет	да	-	да
UserGate UTM 7	да	да	да	-	да	-	да	-	да	нет	нет	да	-	да
ViPNet Coordinator HW	да	да	да	-	да	-	да	-	да	нет	-	да	-	да
ViPNet xFirewall	да	да	да	-	да	-	да	-	да	нет	-	да	-	да
Marlin	да	да	да	-	да	-	да	-	да	да	-	да	-	да
S-Terra VPN Gate	да	нет	да	да	да	да	да	да	-	да	-	нет	-	да
SNR	нет	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да

Тип МЭ	Number	Name	Action	Protocol	Source	Source Port	Destination	Destination Port	Service	Description (remark)	Hit Count	Status (enable/disable)	UUID	Additional
Континент Криптошлюз	нет	да	да	-	да	-	да	-	да	нет	нет	да	-	да
Континент Криптокоммутатор	нет	да	да	-	да	-	да	-	да	нет	нет	да	-	да
Континент Детектор атак	нет	да	да	-	да	-	да	-	да	нет	нет	да	-	да
Континент v.4 Узел безопасности	да	да	да	-	да	-	да	-	да	да	нет	да	-	да
Континент v.4 Узел безопасности с ЦУС	да	да	да	-	да	-	да	-	да	да	нет	да	-	да
Бифорком, коммутаторы серии CS2100	да	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да
Linux	нет	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да
Astra Linux	нет	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да
Debian	нет	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да
Red OS	нет	нет	да	да	да	да	да	да	-	нет	нет	нет	-	да
Примечания: «да» – реализовано; «нет» – не реализовано; «-» – не поддерживается устройством														

Таблица 5 – Поддерживаемые дополнительные данные отчета «Правила МЭ»

Тип МЭ	Inbound Interface	Outbound Interface	Application	User	Last change	Creator	Time Range	Logging
Cisco ASA	-	-	-	да	да	-	да	да
Cisco ASA Context	-	-	-	нет	нет	-	да	да
Cisco PIX	-	-	-	нет	нет	-	да	да
Cisco Firepower Device	да	да	да	нет	нет	-	да	да
Cisco FTD с контролем файлов по SSH	да	да	да	нет	нет	-	да	да
Cisco IOS	-	-	-	нет	нет	-	нет	да
Cisco IOS XE	-	-	-	нет	нет	-	нет	нет

Тип МЭ	Inbound Interface	Outbound Interface	Application	User	Last change	Creator	Time Range	Logging
Cisco IOS XR	-	-	-	нет	нет	-	нет	нет
Check Point Gateway	-	-	-	да	да	да	да	да
Check Point GAiA с контролем файлов по SSH	-	-	-	нет	нет	-	нет	да
Check Point GAiA Embedded с контролем файлов по SSH	-	-	-	нет	нет	-	нет	да
H3C	-	-	-	-	-	-	да	да
Huawei VRP	-	-	-	-	-	-	нет	нет
Eltex MES	-	-	-	да	да	-	да	да
Eltex ESR	-	-	-	да	да	-	нет	нет
Eltex WLC	-	-	-	да	да	-	нет	нет
Dionis NX 1.1	-	-	-	нет	нет	-	нет	да
Dionis NX 1.2	-	-	-	нет	нет	-	нет	да
Dionis-NX 2.0	-	-	-	нет	нет	-	нет	да
Файл конфигурации Dionis-NX	-	-	-	нет	нет	-	нет	да
Fortinet FortiGate	да	да	нет	да	да	-	да	нет
Fortinet FortiGate VDOM (auto)	да	да	нет	да	да	-	да	нет
UserGate UTM 5	да	да	нет	да	да	-	да	нет
UserGate UTM 6	да	да	нет	да	да	-	да	нет
UserGate UTM 7	да	да	нет	да	да	-	да	нет
ViPNet Coordinator HW	-	-	-	-	-	-	-	-
ViPNet xFirewall	-	-	-	-	-	-	-	-
Marlin	да	да	нет	-	-	-	-	да
S-Terra VPN Gate	-	-	-	нет	нет	-	нет	да
SNR	-	-	-	нет	нет	-	да	нет
Континент Криптошлюз	-	-	нет	-	-	-	-	-
Континент Криптокоммутатор	-	-	нет	-	-	-	-	-
Континент Детектор атак	-	-	нет	-	-	-	-	-

Тип МЭ	Inbound Interface	Outbound Interface	Application	User	Last change	Creator	Time Range	Logging
Континент v.4 Узел безопасности	-	-	да	нет	нет	-	да	нет
Континент v.4 Узел безопасности с ЦУС	-	-	да	нет	нет	-	да	нет
Бифорком, коммутаторы серии CS2100	-	-	-	нет	нет	-	да	нет
Linux	-	-	-	нет	нет	-	нет	нет
Astra Linux	-	-	-	нет	нет	-	нет	нет
Debian	-	-	-	нет	нет	-	нет	нет
Red OS	-	-	-	нет	нет	-	нет	нет
Примечания: «да» – реализовано; «нет» – не реализовано; «-» – не поддерживается устройством								

4 Входные и выходные данные

4.1 Входные данные

Входные данные вводятся в поля страниц веб-интерфейса или через запросы REST-интерфейса ПК «Efros DO».

Состав и описание входных данных зависят от выполняемых функций ПК «Efros DO» и приведены в пунктах 4.1.1 – 4.1.7.

4.1.1 Данные модуля «Efros NAC»

Входными данными для модуля «Efros NAC» являются параметры настройки протоколов, приведенные в таблице 6.

Таблица 6 – Параметры настройки протоколов

Элемент	Описание
Длительность активной сессии	Поле для ввода времени жизни активной сессии. Активная сессия – это сессия, для которой получено начало «Аудита RADIUS», но остановка «Аудита RADIUS» еще не получена. Параметр используется для сброса активной сессии конечной точки при отсутствии остановки «Аудита RADIUS» для подсчета количества лицензий функционального модуля «Efros NAC»
*Группа полей протокола TACACS+	
Используемый порт	Порт для протокола TACACS+. По умолчанию содержит значение 49
*Группа полей протокола RADIUS	
Прослушивание пакетов аутентификации	Содержит поля: — IP-адреса прослушиваемых серверов; — номер порта прослушивания пакетов аутентификации. По умолчанию прослушиваются все сервера в сети (значение «*») и порт прослушивания – 1812
Прослушивание пакетов учета	Содержит поля: — IP-адреса прослушиваемых серверов; — номер порта прослушивания пакетов учета. По умолчанию прослушиваются все сервера в сети (значение «*») и порт прослушивания – 1813

4.1.2 Данные модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA», «Efros CM» и «Efros DNS»

Входными данными для модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA», «Efros CM» и «Efros DNS» являются:

1) Настройки:
   - сетевых устройств, серверов, виртуальных инфраструктур и групп данных объектов.
2) Данные, зависящие от состава включенных при настройке ПК внешних модулей для работы с устройствами:
   - принятые по протоколу Telnet, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc854);
   - принятые по протоколу SSH, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4251);
   - принятые по протоколу SCP;
   - принятые по протоколу HTTPS, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2818);
   - принятые Syslog сообщения, формат данных в соответствии со спецификацией (https://tools.ietf.org/html/rfc3164);
   - принятые по протоколу SNMP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc1155);
   - принятые по протоколу REST;
   - принятые по протоколу Microsoft TDS;
   - принятые по протоколу Oracle .Net;
   - принятые по протоколу PostgreSQL Protocol;
   - принятые по протоколу Firebird Wire Protocol;
   - принятые по протоколу MySQL;
   - принятые по протоколу XML-RPC;
   - принятые по протоколу DNS.

4.1.3 Учетные записи пользователей

Описание параметров, используемых при работе с учетными записями пользователей ПК «Efros DO» и ОЗ, приведены в таблице 7.

Таблица 7 – Состав и описание параметров пользователя ПК «Efros DO» и ОЗ

Элемент	Описание
Тип пользователя	Локальный пользователь, пользователь из AD
Логин	Текстовый параметр. Если пользователь является: — локальным пользователем ПК «Efros DO», то параметр задается путем ввода логина вручную; — пользователем AD, то параметр задается путем выбора логина из списка пользователей AD
Пароль	Текстовый параметр. Задается в ПК «Efros DO» только для локальных пользователей. Пароль должен соответствовать требованиям парольной политики ПК «Efros DO»
Статус пользователя	Одно из положений переключателя: — «Активен» – пользователю разрешен доступ в комплекс или к устройствам в соответствии с заданными в ПК «Efros DO» правами; — «Неактивен» – пользователю закрыт доступ в комплекс или к устройствам, контролируемым ПК «Efros DO»
Список доступных объектов	Параметр устанавливается только для пользователя ОЗ. Список доступных ОЗ и права доступа формируются путем выбора из общего списка
Группы пользователя	Выбор группы пользователей из списка

4.1.4 Данные для интеграции с доменной службой AD

Описание параметров, вводимых для настройки работы ПК «Efros DO» с доменной службой AD, приведено в таблице 8.

Таблица 8 – Параметры настройки работы ПК «Efros DO» с доменной службой AD

Элемент	Описание
Название	Поле для ввода названия соединения
Домен/IP-адрес	Поле для ввода имени или IP-адреса домена, к которому подключается сервер ПК «Efros DO»
Подразделение (OU)	Поле для ввода учетной записи сервера ПК «Efros DO» в определенном подразделении. Строка OU читается сверху

Элемент	Описание
	вниз без относительных уникальных имен и разделяется символом «/». Например, «Computers/Servers/Unix»
Серверы аутентификации	Поле для ввода IP-адреса или DNS имени сервера аутентификации
Альтернативное имя группы	Альтернативное имя группы
Блок «Ввод в домен»	
Логин	Поле для ввода логина пользователя, настраивающего подключение
Пароль	Поле для ввода пароля пользователя, настраивающего подключение

4.1.5 Данные учетных записей ACO модуля «Efros NAC»

Описание параметров, используемых при работе с учетными записями ACO в модуле «Efros NAC», приведено в таблице 9.

Таблица 9 – Состав и описание параметров ACO в модуле «Efros NAC»

Элемент	Описание
Название	Поле для ввода названия ACO
Описание	Текстовый параметр
IP-адрес или список подсетей	Текстовый параметр (IP-адрес или диапазон IP-адресов ACO)
Тип протокола	Для каждого типа протокола «TACACS+» и «RADIUS» указывается: — одно из значений переключателя «Включен»/«Выключен» (протокол используется/не используется); — текстовый параметр – значение разделяемого ключа (указывается только для используемого протокола)
Список групп ACO	Список формируется путем выбора из списка групп ACO модуля «Efros NAC»

4.1.6 Данные записей клиентского оборудования из модуля «Efros NAC»

Описание параметров, используемых при работе с учетными записями конечных точек, и проходящих аутентификацию в сети по MAC-адресу учетной записи в модуле «Efros NAC», приведено в таблице 10.

Таблица 10 – Состав и описание параметров конечных точек в модуле «Efros NAC»

Элемент	Описание
MAB	Одно из положений переключателя: — «Запретить MAB» ( ) – КО запрещена аутентификация в сети по MAC-адресу; — «Разрешить MAB» ( ) – КО разрешена аутентификация в сети по MAC-адресу. По умолчанию установлено положение «Запретить MAB»
Название	Текстовое поле для ввода названия КО
Описание	Текстовый параметр
MAC-адрес	Текстовый параметр (MAC-адрес устройства)
Метки	Параметр фильтрации, создаваемый пользователем
Список групп конечных точек	Список формируется путем множественного выбора из списка групп конечных модуля «Efros NAC» согласно назначенным меткам

4.1.7 Данные SSL-сертификатов

Доверенные сертификаты добавляются в ПК «Efros DO» путем импорта из файла формата .pem. При импорте указываются текстовые параметры доверенного сертификата: название и описание.

Системные сертификаты добавляются в ПК «Efros DO» либо автоматически после привязки к созданному ранее запросу сертификата, либо путем импорта уже имеющегося в организации системного сертификата в БД ПК «Efros DO» (аналогично импорту доверенных сертификатов).

При привязке системного сертификата выполняется импорт сертификата из файла формата .pem, при этом указывается название сертификата, а также указывается тип использования сертификата[2] «Используется для WEB» – для установки доверенного соединения при доступе к веб-приложению ПК «Efros DO».

[2] Использование системного сертификата для установки доверенного соединения при доступе устройств в сеть возможно после предварительной настройки TLS (Контроль доступа → Разрешенные протоколы → Настройки TLS). В данном случае, после привязки сертификата появится вариант использования EAP

При привязке или импорте системного сертификата автоматически определяется соответствующий ему доверенный сертификат.

Описание параметров, указываемых при создании запроса сертификата, приведено в таблице 11.

Таблица 11 – Состав и описание параметров запроса сертификата

Элемент	Описание
Название	Текстовое поле для ввода названия запроса сертификата
Данные субъекта	
Город, Общее имя, Страна, Организация, Подразделение, Область	Текстовые параметры
Дополнительное имя субъекта (SAN)	Список альтернативных имен. Каждому имени соответствует его тип: «DNS», «IP-адрес», «URI» или «Директория», и значение параметра

4.2 Выходные данные

4.2.1 Данные из журнала «События»

Выгрузка данных из журнала «События», зафиксированных ПК «Efros DO», осуществляется по запросу администратора в файлы формата CSV и XLSX. Перед выгрузкой пользователь может провести поиск и фильтрацию данных в журнале.

4.2.2 Данные модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA», «Efros CM» и «Efros DNS»

Выходными данными для модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA», «Efros CM» и «Efros DNS» являются:

1) Сохраненные в БД отчеты о конфигурации и состоянии контролируемых устройств.
2) Данные (состав выходных данных зависит от состава включенных при настройке ПК «Efros DO» внешних модулей):
   — переданные по протоколу Telnet, формат данных в соответствии со

спецификацией для протокола (https://courses.cs.washington.edu/courses/cse461/14sp/homework/rfc854-modified.html);

- переданные по протоколу SSH, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc4251);
- переданные по протоколу SCP;
- принятые по протоколу HTTPS, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc2818);
- переданные по протоколу SMTP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc5321);
- переданные по протоколу Syslog, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc3164);
- переданные по протоколу SNMP, формат данных в соответствии со спецификацией для протокола (https://tools.ietf.org/html/rfc1155);
- переданные по протоколу Microsoft Exchange Web Services Managed API (при отправке через MS Exchange), формат данных в соответствии со спецификацией для протокола (https://learn.microsoft.com/ru-ru/exchange/client-developer/exchange-web-services/explore-the-ews-managed-api-ews-and-web-services-in-exchange);
- переданные по протоколу REST;
- переданные по протоколу Microsoft TDS;
- переданные по протоколу Oracle .Net;
- переданные по протоколу PostgreSQL protocol;
- переданные по протоколу Firebird Wire Protocol;
- переданные по протоколу MySQL;
- переданные по протоколу XML-RPC;
- переданные по протоколу DNS.

Приложение А
Оборудование, поддерживаемое серверной частью ПК «Efros DO», в зависимости от установленной лицензии

А.1 Перечень типов устройств, поддерживаемых функциональными модулями «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»

Перечень типов устройств, поддерживаемых функциональными модулями «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM», приведен в таблице 12.

Примечание – В таблице использованы следующие условные обозначения:

- «да» – поддерживается, требуется дополнительная лицензия;
- «НЛ» – не лицензируется, нет ограничений по лицензиям;
- «нет» – не поддерживается;
- «-» – неприменимо для данного типа лицензии.

Таблица 12 – Типы устройств, поддерживаемые модулями «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Сетевые устройства					
3Com OS	да	нет	-	да	нет
Allied-Telesis AT-GS950	да	нет	-	нет	нет
Avaya	да	нет	-	нет	нет
Check Point GAiA	да	нет	-	да	нет
Check Point GAiA с контролем файлов по SSH	да	да	-	да	нет
Check Point GAiA Embedded	да	нет	-	да	нет
Check Point GAiA Embedded с контролем файлов по SSH	да	да	-	да	нет
Check Point SmartCenter	да	да	-	нет	нет
Check Point R80 Management Server	да	нет	-	нет	нет
Check Point Domain Management Server	да	нет	-	нет	нет

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Check Point Gateway	да	да	-	нет	да
Check Point SecurePlatform	да	нет	-	да	нет
Check Point Maestro Orchestrator	да	нет	-	да	нет
Cisco ACI	да	нет	-	нет	нет
Cisco ACS	да	нет	-	да	нет
Cisco ASA	да	да	-	да	да
Cisco ASA Context	да	да	-	нет	нет
Cisco ASA Context (Auto)	да	да	-	нет	нет
Файлы конфигураций ASA	НЛ	НЛ		НЛ	НЛ
Файл конфигурации ASA	да	да	-	нет	нет
Cisco IronportAsyncOS	да	нет	-	да	нет
Cisco CatOS	да	нет	-	нет	нет
Cisco FMC	НЛ	НЛ	-	да	нет
Cisco Firepower Device	да	да	-	нет	нет
Cisco FTD	да	нет	-	да	нет
Cisco FTD с контролем файлов по SSH	да	да	-	да	нет
Cisco FWSM Module	да	нет	-	да	нет
Cisco IOS	да	да	-	да	нет
Cisco IOS XE	да	да	-	да	нет
Cisco IOS XR	да	да	-	нет	нет
Cisco IPS	да	нет	-	нет	нет
Cisco NX-OS	да	нет	-	да	нет
Cisco PIX	да	да	-	да	нет
Cisco SMB	да	нет	-	да	нет
Cisco WAP	да	нет	-	нет	нет
Cisco WLC	да	нет	-	да	нет
Crossbeam XOS v.9	да	нет	-	нет	нет
Phoenix contact	да	нет	-	нет	нет
H3C	да	да	-	нет	нет

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Dionis-LX	да	нет	-	нет	нет
Dionis-NX 1.1	да	да	-	нет	нет
Dionis-NX 1.2	да	да	-	нет	нет
Dionis-NX 2.0	да	да	-	нет	нет
Файлы конфигураций Dionis	НЛ	НЛ	-	НЛ	НЛ
Файл конфигурации Dionis-LX	да	нет	-	нет	нет
Файл конфигурации Dionis-NX	да	да	-	нет	нет
D-Link DES	да	нет	-	да	нет
D-Link DGS	да	нет	-	да	нет
D-Link DGS 1210	да	нет	-	да	нет
D-Link DGS 3130/3630	да	нет	-	да	нет
Edge-Core ECS	да	нет	-	нет	нет
Eltex ESR	да	да	-	да	нет
Eltex ME	да	нет	-	да	нет
Eltex MES	да	да	-	да	нет
Eltex MES 24xx	да	нет	-	да	нет
Eltex WLC	да	да	-	нет	да
Eltex WOP/WEP	да	нет	-	нет	нет
Extreme 220 series	да	нет	-	нет	нет
ExtremeXOS	да	нет	-	нет	нет
Fortinet FortiGate	да	да	-	да	нет
Fortinet FortiGate VDOM	да	нет	-	да	нет
Fortinet FortiGate VDOM (auto)	да	да	-	нет	нет
Fortinet FortiSwitch	да	нет	-	да	нет
Fortinet FortiWLC	да	нет	-	да	нет
Hirschmann MAR	да	нет	-	да	нет
HP Aruba	да	нет	-	да	нет
HP BladeSystem	да	нет	-	да	нет
HP Comware Switch	да	нет	-	да	нет

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
HP Procurve	да	нет	-	да	нет
HP Virtual Connect	да	нет	-	нет	нет
Huawei VRP	да	да	-	да	нет
Juniper JunOS	да	нет	-	да	нет
Korenix JetNet	да	нет	-	нет	нет
Lenovo Cumulus	да	нет	-	нет	нет
Lenovo ENOS 8.4	да	нет	-	нет	нет
Lenovo FabricOS 8.x	да	нет	-	нет	нет
Marlin	да	да	-	нет	нет
Mikrotik RouterOS	да	нет	-	да	нет
Moxa EDS	да	нет	-	да	нет
Moxa MGate	да	нет	-	да	нет
Moxa Nport 5150	да	нет	-	нет	нет
Nateks NX-3400	да	нет	-	нет	нет
Nateks NX-5100	да	нет	-	нет	нет
Nateks NXI-3030	да	нет	-	нет	нет
Nateks NXI-3050	да	нет	-	нет	нет
КриптоПро TLS шлюз	да	нет	-	нет	нет
NS Gate NIS	да	нет	-	нет	нет
Palo Alto Pan-OS 7	да	нет	-	да	нет
Palo Alto Pan-OS 9	да	нет	-	да	нет
PKCC OmniAccess 700	да	нет	-	нет	нет
PKCC OmniSwitch 6850	да	нет	-	нет	нет
PKCC OmniSwitch 7710	да	нет	-	нет	нет
PKCC OmniSwitch 7750	да	нет	-	нет	нет
PKCC OmniSwitch 9000	да	нет	-	нет	нет
PKCC Onyx	да	нет	-	нет	нет
QTech QSW	да	нет	-	нет	нет
Raisecom ISCOM	да	нет	-	нет	нет

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Rockwell Cisco IOS	да	нет	-	да	нет
Tfortis PSW	да	нет	-	нет	нет
Siemens Scalance X-300 series	да	нет	-	да	нет
Siemens Scalance X-400 series	да	нет	-	да	нет
S-Terra VPN Gate	да	да	-	нет	нет
SNR	да	да	-	нет	нет
UserGate UTM 5	да	да	-	да	нет
UserGate UTM 6	да	да	-	да	нет
UserGate UTM 7	да	да	-	да	нет
VipNet Coordinator HW	да	да	-	да	нет
VipNet xFirewall	да	да	-	да	нет
VipNet Prime	да	нет	-	нет	нет
Weidmuller	да	нет	-	да	нет
WatchGuard Fireware OS	да	нет	-	нет	нет
WatchGuard Fireware XTM OS	да	нет	-	нет	нет
Zelax M-1-MEGA	да	нет	-	нет	нет
Zelax ZES	да	нет	-	нет	нет
ZyXEL ZyNOS	да	нет	-	да	нет
Континент Криптошлюз	да	да	-	нет	нет
Континент Криптокоммутатор	да	да	-	нет	нет
Континент Детектор атак	да	да	-	нет	нет
Континент v.4 Api коннектор	НЛ	НЛ	-	НЛ	НЛ
Континент v.4 Узел безопасности	да	да	-	нет	нет
Континент v.4 Узел безопасности с ЦУС	да	да	-	нет	нет
Бифорком, коммутаторы серии CS2100	да	да	-	нет	нет
Полигон Арлан	да	нет	-	нет	нет
Полигон ИнЗер	да	нет	-	нет	нет
Операционные системы					
Windows	да	нет	да	да	-

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Windows Agent 2000/XP	нет	нет	да	нет	-
Linux	да	да	да	да	-
AIX	да	нет	да	нет	-
HP-UX	да	нет	да	нет	-
Alt Linux	да	нет	да	да	-
Astra Linux	да	да	да	да	-
Debian	да	да	да	да	-
FreeBSD	да	нет	да	нет	-
Red OS	да	да	да	да	-
SunOS	да	нет	да	нет	-
XenServer	нет	нет	да	нет	-
Active Directory Domain	нет	нет	да	нет	-
Виртуализация					
vCenter VCSA	нет	нет	НЛ	нет	-
vCenter Windows	да	нет	НЛ	да	-
Host	нет	нет	да	да	-
Host с контролем целостности по SSH	нет	нет	да	да	-
Host с контролем целостности по HTTPS	нет	нет	да	да	-
ESXi ОС с контролем целостности по SSH	нет	нет	да	нет	-
ESXi ОС с контролем целостности по HTTPS	нет	нет	да	нет	-
Standalone ESXi с контролем целостности по SSH	нет	нет	да	да	-
Standalone ESXi с контролем целостности по HTTPS	нет	нет	да	да	-
Virtual Machine Manager	нет	нет	нет	нет	-
Hyper-V хост	нет	нет	нет	нет	-
Hyper-V хост с контролем целостности	нет	нет	нет	нет	-
Standalone Hyper-v	нет	нет	нет	нет	-
KVM	нет	нет	да	нет	-

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
zVirt	нет	нет	НЛ	да	-
zVirt Host	нет	нет	да	нет	-
zVirt Host с контролем целостности по SSH	нет	нет	да	да	-
Proxmox	нет	нет	НЛ	нет	-
Proxmox Хост	нет	нет	да	нет	-
Proxmox Хост с контролем целостности по SSH	нет	нет	да	нет	-
Tionix	нет	нет	НЛ	нет	-
Tionix Linux	нет	нет	НЛ	нет	-
Tionix Гипервизор	нет	нет	да	нет	-
Скала-Р	нет	нет	НЛ	нет	-
Скала-Р Кластер	нет	нет	НЛ	нет	-
Скала-Р Виртуальная среда	нет	нет	НЛ	нет	-
Скала-Р Хост	нет	нет	да	нет	-
Скала-Р Хост с контролем целостности по SSH	нет	нет	да	нет	-
Basis	нет	нет	НЛ	нет	-
Basis Кластер	нет	нет	НЛ	нет	-
Basis Виртуальная среда	нет	нет	НЛ	нет	-
Basis Хост	нет	нет	да	нет	-
Basis Хост с контролем целостности по SSH	нет	нет	да	нет	-
РЕД Виртуализация	нет	нет	НЛ	нет	-
РЕД Виртуализация Host	нет	нет	Да	нет	-
РЕД Виртуализация Host с контролем целостности по SSH	нет	нет	да	да	-
Docker	нет	нет	да	да	-
Docker Astra	нет	нет	да	да	-
Docker Debian	нет	нет	да	да	-
Docker Linux	нет	нет	да	да	-
Docker Red OS	нет	нет	да	да	-

Тип устройства	Лицензия				
	Efros NA	Efros FA	Efros ICC	Efros VC	Efros CM
Kubernetes cluster	нет	нет	да	да	-
Прикладное программное обеспечение					
Firebird	-	-	да	нет	-
Jatoba	-	-	да	нет	-
Microsoft SQL	-	-	да	нет	-
MySQL	-	-	да	нет	-
Oracle	-	-	да	нет	-
PostgreSQL	-	-	да	нет	-
PostgreSQL Database	-	-	да	нет	-
UiPath	-	-	да	нет	-
Primo RPA	-	-	да	нет	-
SCADA	-	-	да	нет	-
ПЛК	-	-	да	-	-

A.2 Перечень словарей RADIUS и оборудование, поддерживаемых функциональным модулем «Efros NAC»

Функциональный модуль «Efros NAC» поддерживает следующие словари RADIUS:

- 3Com;
- 3GPP;
- Acme;
- Airspace;
- Alcatel;
- Alteon;
- Altiga;
- Alvarion;
- Checkpoint;
- Cisco;
- Crypto-pro;

- Efros ACS;
- Eltex;
- Erisson;
- Extreme;
- Fortinet;
- H3C;
- HP;
- Huawei;
- Juniper;
- Microsoft;
- Microtik;
- Motorola;
- Nokia.

В таблице 13 приведен перечень оборудования, поддерживаемого функциональным модулем «Efros NAC», с указанием поддерживаемых функций:

- 802.1X – поддержка аутентификации доступа к сети с использованием протокола 802.1X;
- Mac Auth – поддержка аутентификации доступа к сети с MAC адреса;
- VPN – поддержка аутентификации доступа к VPN серверу по протоколу RADIUS;
- RADIUS Downloadable ACL – поддержка использования ACL, загружаемых в процессе авторизации;
- RADIUS Preconfigured ACL – поддержка использования ACL, заранее созданные на оборудовании;
- Change of Authorization – поддержка механизма изменения авторизации (CoA);
- RADIUS Device Administration – поддержка протокола RADIUS для доступа администраторов на устройство;
- TACACS Device Administration – поддержка протоколаTACACS для доступа администраторов на устройство.

Примечание – В таблице использованы следующие условные обозначения:

- «+» – поддерживается;
- «+/-» – частично поддерживается;

— «-» – не поддерживается.

Таблица 13 – Оборудование, поддерживаемое модулем «Efros NAC»

Устройство	802.1X	MAC Authentication	VPN	RADIUS Downloadable ACL	RADIUS Preconfigured ACL	CoA	RADIUS Device Administration	TACACS Device Administration
Коммутаторы CISCO IOS и IOS XE	+	+			+	+	+	+
Маршрутизаторы CISCO IOS и IOS XE			+	+	+	+	+	+
МСЭ CISCO ASA			+	+	+	+	+	+
Коммутаторы CISCO Nexus								-
StrongSwan			+					
OpenVPN (с плагином openvpn-radiusplugin)			+					
pfSense			+	+				
CheckPoint			+					
WiFi контроллеры CISCO WLC	+	+		+		+	+	
Коммутатор Extreme Summit X440G2	+	+		-	-		+	+/-
Маршрутизатор Juniper Networks MX							+	-
Коммутатор Juniper Networks QFX	+	+		+	+		+	-
Коммутаторы Eltex MES23xx/33xx/35xx/53xx	+	+		+	+		+	+/-
Коммутаторы Eltex MES 24xx/34xx	+	+	-	+	+	-		+
Маршрутизаторы ESR			+	-			-	
WiFi контроллеры Eltex WLC	+	+						
Коммутатор Qtech QSW-4700	+	+		+	+			+
Коммутатор Huawei S5735-L24P4S-A1							+	+/-

A.3 Перечень оборудования, поддерживаемого функциональным модулем «Efros NFA»

Функциональный модуль «Efros NFA» поддерживает следующее оборудование:

- Cisco;
- D-Link;
- Eltex;
- Huawei;
- Mikrotik.

Перечень сокращений

ACL	–	Access Control List
AD	–	Active Directory
API	–	Application Programming Interface
CM	–	Change Manager
CoA	–	Change of Authorization
CPMI	–	Common Management Information Protocol
CSV	–	Comma-Separated Values
DES	–	Data Encryption Standard
DNS	–	Domain Name System
GRE	–	Generic Routing Encapsulation
HTTP	–	HyperText Transfer Protocol
HTTPs	–	HyperText Transfer Protocol Secure
ICC	–	Integrity Check Compliance
IDS	–	Intrusion Detection System
IP	–	Internet Protocol
IPFIX	–	Internet Protocol Flow Information Export
IPS	–	Intrusion Prevention System
LDAP	–	Lightweight Directory Access Protocol
MAB	–	MAC Authentication Bypass
MAC	–	Media Access Control
NA	–	Network Assurance
NAC	–	Network Access Control
NAT	–	Network Address Translation
NFA	–	Network Flow Analysis
PBR	–	Policy-based routing
RADIUS	–	Remote Authentication in Dial–In User Service
SCP	–	Secure Copy
SFTP	–	Secure File Transfer Protocol
SNMP	–	Simple Network Management Protocol
SQL	–	Structured Query Language
SSH	–	Secure Shell

SSL	–	Secure Sockets Layer
TACACS+	–	Terminal Access Controller Access Control System plus
TDS	–	Tabular Data Stream
TELNET	–	TELecommunication NETwork
TLS	–	Transport Layer Security
URI	–	Uniform Resource Identifier
UUID	–	Universally Unique Identifier
VC	–	Vulnerability Control
VM	–	Virtual Machine
VPN	–	Virtual Private Network
XML	–	eXtensible Markup Language
АО	–	Акционерное общество
АСО	–	Активное сетевое оборудование
АСУ ТП	–	Автоматизированная система управления технологическим процессом
БД	–	База данных
БДУ	–	База данных уязвимостей
ЗАО	–	Закрытое акционерное общество
ИБ	–	Информационная безопасность
КО	–	Клиентское оборудование
МЭ	–	Межсетевой экран
НПО	–	Научно-производственное объединение
ОАО	–	Открытое акционерное общество
ОЗ	–	Объект защиты
ООО	–	Общество с ограниченной ответственностью
ОС	–	Операционная система
ПК	–	Программный комплекс
ППО	–	Прикладное программное обеспечение
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно-вычислительная машина