GIS ГАЗИНФОРМ СЕРВИС

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

Санкт-Петербург, 2023

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 (далее – ИБ):

- контроль конфигураций и топологии сети;
- контроль целостности и проверки соответствия хостов и конечных точек;
- оптимизация и настройка межсетевых экранов (далее – 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.

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, предоставляющий полный контроль над автоматизацией процессов информационной безопасности (далее – ИБ);
- 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»);
- микросервис аутентификации и авторизации пользователей ПК «Efros DO»;
- микросервис лицензирования;
- микросервис объектов защиты;
- микросервис сбора метрик ИБ;
- микросервис расписаний;
- микросервис событий и уведомлений;
- микросервис маршрутизации запросов;

— модуль обмена данными Apache Kafka;

— модуль хранения данных OpenSearch;

— подсистема хранения данных: система управления базами данных (далее – СУБД).

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».

1.3. Функциональные возможности программы

ПК «Efros DO» реализует следующие функциональные возможности:

— единая точка доступа к функциям системы и модулям интеграции;

— получение, обработка, интеграция и хранение данных, полученных из событий по объектам защиты (далее – 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;

— управление ролями пользователей комплекса;

— 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».

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:
   - просмотр ОЗ;
   - инвентаризация параметров сети и управление несконфигурированными ОЗ (добавление/удаление ОЗ);
   - просмотр карты сети ОЗ;
   - база знаний по ОЗ;
   - векторы атак;
   - ведение списка контролируемого клиентского оборудования (конечных точек сети и их групп);
   - сканирование сети.
2) Контроль устройств:
   - настройка доступа к объектам сети/группам объектов сети;
   - проверка безопасности;
   - проверка МЭ;
   - настройка профилей подключения;
   - 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 устройствами/группами устройств;
   - управление сетевыми пользователями/группами сетевых пользователей, имеющих доступ к активному сетевому оборудованию (далее – АСО);
   - настройка политик доступа;
   - настройка условий доступа;
   - настройка профилей авторизации;
   - настройка профилей оборудования;
   - редактирование разрешенных протоколов аутентификации;
   - редактирование набора команд;
   - настройка подключения к сервисам протоколов TACACS+ и RADIUS;
   - загрузка ACL;
   - словари атрибутов;
   - создание и управление гостевыми порталами.
4) Администрирование:
   - управление пользователями/группами пользователей;
   - управление лицензиями на подключаемые модули;
   - просмотр системных событий;
   - настройка планировщика задач и событий;
   - ведение списка корневых, серверных и клиентских сертификатов, создание запросов на сертификаты.
5) Управление настройками ПК «Efros DO»:
   - настройка домена Active Directory (далее – AD);
   - управление триггерами Flow;
   - аутентификация АСО;
   - управление хранением данных;
   - настройка почтовых серверов;
   - импорт данных.
6) 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 для аутентификации, авторизации и учета действий пользователя на сетевых устройствах:
   - протоколы TACACS+ и/или RADIUS.
2) Установлены внешние модули, отвечающие за активный аудит сетевого оборудования, серверных и клиентских операционных систем (далее – 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 отправки syslog-сообщений и syslog-сервера (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.
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 активный контроль сетевого оборудования, серверных и клиентских ОС, автоматизированных систем управления технологическим процессом

(АСУ ТП), виртуальных сред, а также анализ правил МЭ 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 (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 Мега, 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 ESR, ME, MES, MES2428, 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));
- СУБД Microsoft (MS SQL 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);
- ООО «ИнСАТ» (MasterSCADA);
- ФГУП «ЭЗАН» (SCADA-система «Соната»);
- 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).

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 и прикладного программного обеспечения (далее – ППО);
- контроль целостности файлов ОС, виртуализации и ППО;
- проверки соответствия безопасности ОС, виртуализации 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 (далее – 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.

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 следующие функциональные возможности ПК «Efros DO»:

- автоматизация управления жизненным циклом правил МЭ.

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).

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

Сетевые пользователи 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	Привилегии	Права	Описание
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»
	Лицензии	Просмотр/ Управление	Доступ к разделу: — Администрирование/Лицензии
	Сертификаты	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Сертификаты
	Планировщик	Просмотр/ Управление	Доступ к разделу: — Администрирование/ Планировщик
Общие настройки	Основные функции**	Управление	Доступ к разделам: — Мониторинг; — Объекты сети; — Отчеты (личные). 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
	Векторы атак	Просмотр/ Управление	Доступ к разделу: — Объекты сети/Векторы атак
	Конечные точки	Просмотр/ Управление	Доступ к разделу: — Объекты сети/Конечные

Группа привилегий	Привилегии	Права	Описание
			точки
	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-адрес
	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
	Журналы событий системы**	Управление	Доступ к разделу: — События
Центр задач	Администрирование	Просмотр/ Управление	Доступ к разделу: — «Центр задач»
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»)
	Общие / Импорт данных		Доступ к разделу: — Настройки/Группа «Общие»/ Импорт данных
*«Просмотр»: чтение конфигураций, состояний ОЗ; «Управление»: просмотр, редактирование конфигураций, изменение прав пользователей			

Группа привилегий	Привилегии	Права	Описание
**Привилегии включают в себя право только на управление			

После установки и настройки ПК «Efros DO» в БД 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 прикладному ПО

Элемент	Параметры		
Количество объектов защиты (ОЗ)	До 500	До 1000	До 2000*
Требования к программному обеспечению			
ОС	Astra Linux Special Edition (v. 1.6, v.1.7), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.); Astra Linux Common Edition (v.2.12); Альт 10 Server; РЕД ОС 7.3 Муром, сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
Поддерживаемые системы управления базами данных (СУБД)	СУБД PostgreSQL 13; СУБД «Jatoba»		
Прикладное ПО	Docker 18.03.0 и выше; Docker-compose v2.9.0; Confluent Kafka 5.5.0		
Требования к аппаратному обеспечению			
Процессор	12 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память, не менее Гб	от 16 Гб	от 32 Гб	от 64 Гб
Жесткий диск, Гб (ПК + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер ПК, Гб	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД, Гб	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		
Требования для функционирования модуля «Efros NFA»			
Netflow v9+, IPFIX	порт 2056		
sFlow	порт 6343		
Netflow v5	порт 2055		

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

Элемент	Параметры
Требования для функционирования модулей «Efros NA», «Efros FA», «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
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); 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)	

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 («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»).

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

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 (таблица 3).

Таблица 3 – 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» и «Efros CM»

Входными данными для модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA» и «Efros CM» 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.

4.1.3 Учетные записи пользователей

Описание параметров, используемых при работе с учетными записями пользователей ПК «Efros DO» и ОЗ приведены в таблице 4.

Таблица 4 – Состав и описание параметров пользователя ПК «Efros DO»

Элемент	Описание
Тип пользователя	Локальный пользователь
Логин	Текстовый параметр
Пароль	Текстовый параметр. Задается в ПК «Efros DO» только для локальных пользователей. Пароль должен соответствовать требованиям парольной политики ПК «Efros DO»
Статус пользователя	— «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 5.

Таблица 5 – 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 вниз без относительных уникальных имен и разделяется символом «/». Например, «Computers/Servers/Unix»
Серверы аутентификации	Поле для ввода IP-адреса или DNS имени сервера аутентификации

Элемент	Описание
Альтернативное имя группы	Альтернативное имя группы
Блок «Ввод в домен»	
Логин	Поле для введения логина пользователя, настраивающего подключение
Пароль	Поле для введения 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» (таблица 6).

Таблица 6 – Состав и описание параметров ACO в модуле «Efros NAC»

Элемент	Описание
Название	Текстовый параметр
Описание	Текстовый параметр
IP-адрес или список подсетей	Текстовый параметр (IP-адрес или диапазон IP-адресов устройства)
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 клиентского оборудования (КО), аутентифицирующегося в сети по MAC-адресу учетной записи в модуле «Efros NAC», приведено в таблице 7.

Таблица 7 – Состав и описание параметров КО в модуле «Efros NAC»

Элемент	Описание
MAB	— «Запретить MAB» () – конечной точке запрещена аутентификация в сети по MAC-адресу;

Элемент	Описание
	— «Разрешить MAB» ( ) – конечной точке разрешена аутентификация в сети по MAC-адресу. По умолчанию установлено положение «Запретить MAB»
Название	Текстовый параметр
Описание	Текстовый параметр
MAC-адрес	Текстовый параметр (MAC-адрес устройства)
Метки	Параметр фильтрации, создаваемый пользователем
Список групп КО	Список формируется путем множественного выбора из списка групп КО модуля «Efros NAC»

4.1.7 Данные SSL-сертификатов

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

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

При привязке серверного 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».

При привязке или импорте серверного сертификата автоматически определяется соответствующий ему корневой сертификат.

Описание параметров, указываемых при создании запроса сертификата, приведено в таблице 8.

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

Таблица 8 – Состав и описание параметров запроса сертификата

Элемент	Описание
Название	Текстовый параметр
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» (в виде файлов)

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

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

Выходными данными для модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros NFA» и «Efros CM» 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.

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
HTTP	–	HyperText Transfer Protocol
HTTPs	–	HyperText Transfer Protocol Secure
ICC	–	Integrity Check Compliance
IP	–	Internet Protocol
IPFIX	–	Internet Protocol Flow Information Export
FA	–	Firewall Assurance
LDAP	–	Lightweight Directory Access Protocol
MAB	–	MAC Authentication Bypass
MAC	–	Media Access Control
NA	–	Network Assurance
NAC	–	Network Access Control
NFA	–	Network Flow Analysis
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 Socket Layer
TACACS+	–	Terminal Access Controller Access Control System plus
TDS	–	Tabular Data Stream
TELNET	–	TELecommunication NETwork
TLS	–	Transport Layer Security

URI	–	Uniform Resource 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
ФГУП	–	Федеральное государственное унитарное предприятие
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно–вычислительная машина

Приложение А

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

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
Сетевые устройства								
1	3Com OS	да\нет	да\нет	-	-	да	-	да/нет
2	Allied-Telesis AT-GS950	да\нет	да\нет	-	-	да	-	да/нет
3	Avaya	да\нет	да\нет	-	-	да	-	да/нет
4	B4com	да\нет	да\нет	-	-	нет	-	да/нет
5	Check Point GAiA	да\нет	да\нет	да	нет	да	-	да/нет
6	Check Point GAiA с контролем файлов по SSH	да\нет	да	да	нет	да	-	да/нет
7	Check Point GAiA Embedded с контролем файлов по SSH	да\нет	да\нет	нет	нет	да	-	да/нет
8	Check Point GAiA Embedded	-	да\нет	нет	нет	да	-	да/нет
9	Check Point Gateway	-	да\нет	да	нет	нет	-	да/нет
10	Check Point R80 Management Server	-	да\нет	нет	нет	нет	-	да/нет
11	Check Point SecurePlatform	да\нет	да\нет	нет	нет	да	-	да/нет
12	Check Point SmartCenter	-	да\нет	нет	нет	нет	-	да/нет
13	Check Point Maestro Orchestrator	-	да\нет	нет	нет	нет	-	да/нет
14	Cisco ACS	-	да\нет	-	-	да	-	-
15	Cisco ASA	да	да	да	нет	да	-	да
16	Cisco ASA Context	-	да	да	нет	нет	-	-
17	Cisco IronportAsyncOS	да\нет	да\нет	-	-	да	-	-
18	Cisco CatOS	-	да\нет	-	-	нет	-	-
19	Cisco FMC	-	да\нет	нет	нет	да	-	-
20	Cisco Firepower Device	-	да\нет	да	нет	нет	-	-

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
21	Cisco FTD	да\нет	да\нет	да	нет	да	-	-
22	Cisco FTD с контролем файлов по SSH	да\нет	да\нет	да	нет	нет	-	-
23	Cisco FWSM Module	да\нет	да\нет	-	-	да	-	-
24	Cisco IOS	да	да\нет	да	нет	да	-	да
25	Cisco IOS XE	да\нет	да\нет	нет	нет	да	-	да
26	Cisco IOS XR	да\нет	да\нет	нет	нет	нет	-	да
27	Cisco IPS	-	да\нет	нет	нет	нет	-	-
28	Cisco NX-OS	да\нет	да\нет	нет	нет	да	-	да/нет
29	Cisco PIX	да\нет	да\нет	да	нет	да	-	да/нет
30	Cisco SMB	да\нет	да\нет	-	-	да	-	да/нет
31	Cisco UCM	-	да\нет	-	-	да	-	-
32	Cisco WAP	да\нет	да\нет	-	-	нет	-	-
33	Cisco WLC	да	да\нет	-	-	да	-	да/нет
34	Crossbeam XOS	-	да\нет	-	-	нет	-	-
35	Dionis-LX	-	да\нет	-	-	нет	-	да/нет
36	Dionis-NX 1.1	-	да\нет	-	-	нет	-	да/нет
37	Dionis-NX 1.2	-	да\нет	-	-	нет	-	да/нет
38	Dionis-NX 2.0	да\нет	да	да	нет	нет	-	да/нет
39	D-Link DES	да\нет	да\нет	-	-	да	-	да/нет
40	D-Link DGS	да\нет	да\нет	-	-	да	-	да/нет
41	D-Link DGS 1210	-	да\нет	-	-	да	-	да/нет
42	D-Link DGS 3130/3630	да\нет	да\нет	-	-	да	-	да/нет
43	Edge-Core ECS	да\нет	да\нет	-	-	нет	-	-
44	Eltex ESR	да	да	да\нет	нет	да	-	да/нет
45	Eltex ME	да\нет	да\нет	нет	нет	да	-	да/нет

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
46	Eltex MES	да	да	да	нет	да	-	да/нет
47	Eltex MES 24xx	да\нет	да\нет	нет	нет	да	-	да/нет
48	Eltex WOP/WEP	-	да\нет	-	-	нет	-	да/нет
49	Extreme 220 series	да\нет	да\нет	-	-	нет	-	да/нет
50	ExtremeXOS	да\нет	да\нет	-	-	нет	-	да/нет
51	Fortinet FortiGate	да\нет	да\нет	да	нет	нет	-	да/нет
52	Fortinet FortiGate VDOM	да\нет	да\нет	да	нет	нет	-	да/нет
53	Fortinet FortiSwitch	да\нет	да\нет	-	-	нет	-	да/нет
54	Fortinet FortiWLC	да\нет	да\нет	-	-	нет	-	да/нет
55	Hirschmann MAR	-	да\нет	-	-	да	-	да/нет
56	HP Aruba	да\нет	да\нет	-	-	да	-	-
57	HP BladeSystem	-	да\нет	-	-	да	-	-
58	HP Comware Switch	-	да\нет	-	-	да	-	-
59	HP Procurve	да\нет	да\нет	нет	нет	да	-	-
60	HP Virtual Connect	да\нет	да\нет	-	-	нет	-	-
61	Huawei VRP	да	да	да	нет	да	-	да/нет
62	Juniper JunOS	да\нет	да\нет	-	-	да	-	да/нет
63	Korenix JetNet	да\нет	да\нет	-	-	нет	-	да/нет
64	Lenovo Cumulus	-	да\нет	нет	нет	нет	-	да/нет
65	Lenovo ENOS 8.4	-	да\нет	нет	нет	нет	-	да/нет
66	Lenovo FabricOS 8.x	-	да\нет	нет	нет	нет	-	да/нет
67	Marlin	-	да\нет	да	нет	нет	-	да/нет
68	Mikrotik RouterOS	да	да\нет	нет	нет	нет	-	да/нет
69	Moxa EDS	да\нет	да\нет	нет	нет	да	-	да/нет
70	Moxa MGate	да\нет	да\нет	-	-	да	-	да/нет
71	Moxa Nport 5150	-	да\нет	нет	нет	нет	-	да/нет

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
72	Nateks NX-3400	да\нет	да\нет	-	-	нет	-	да/нет
73	Nateks NX-5100	да\нет	да\нет	-	-	нет	-	да/нет
74	Nateks NXI-3030	да\нет	да\нет	-	-	нет	-	да/нет
75	Nateks NXI-3050	да\нет	да\нет	-	-	нет	-	да/нет
76	NS Gate NIS	да\нет	да\нет	-	-	нет	-	-
77	Palo Alto Pan-OS 7	да\нет	да\нет	-	-	да	-	-
78	Palo Alto Pan-OS 9	да\нет	да\нет	нет	нет	да	-	-
79	PKCC OmniAccess 700	-	да\нет	-	-	нет	-	да/нет
80	PKCC OmniSwitch 6850	-	да\нет	-	-	нет	-	да/нет
81	PKCC OmniSwitch 7710	-	да\нет	-	-	нет	-	да/нет
82	PKCC OmniSwitch 7750	-	да\нет	-	-	нет	-	да/нет
83	PKCC OmniSwitch 9000	-	да\нет	-	-	нет	-	да/нет
84	PKCC Onyx	-	да\нет	-	-	нет	-	да/нет
85	Phoenix Contact	-	да	-	-	-	-	-
86	QTech QSW	да\нет	да\нет	-	-	нет	-	да/нет
87	Raisecom ISCOM	да\нет	да\нет	-	-	нет	-	-
88	Rockwell Cisco IOS	-	да\нет	нет	нет	да	-	да/нет
89	Siemens Scalance X-300 series	да\нет	да\нет	-	-	да	-	да/нет
90	Siemens Scalance X-400 series	да\нет	да\нет	-	-	да	-	да/нет
91	S-Terra VPN Gate	да\нет	да	да	нет	нет	-	да/нет
92	UserGate UTM 5	да\нет	да\нет	да	нет	нет	-	да/нет
93	UserGate UTM 6	да\нет	да	да	нет	нет	-	да/нет
94	VipNet Coordinator HW	-	да	да	нет	нет	-	да/нет
95	VipNet xFirewall	-	да	да	нет	нет	-	да/нет
96	VipNet Prime	-	да	-	-	-	-	-

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
97	WatchGuard Fireware OS	-	да\нет	-	-	нет	-	да/нет
98	WatchGuard Fireware XTM OS	-	да\нет	-	-	нет	-	да/нет
99	Zelax M-1-MEGA	-	да\нет	-	-	нет	-	да/нет
100	Zelax ZES	да\нет	да\нет	-	-	нет	-	да/нет
101	ZyXEL ZyNOS	да\нет	да\нет	-	-	да	-	да/нет
102	H3C	-	да	-	-	-	да	-
103	Код Безопасности Континент	-	да\нет	нет	нет	нет	-	-
104	КриптоПро TLS шлюз	-	да\нет	нет	нет	нет	-	да/нет
105	Полигон Арлан	да\нет	да\нет	нет	нет	нет	-	-
106	Полигон ИнЗер	да\нет	да\нет	нет	нет	нет	-	-
Операционные системы								
1	Windows	-	нет	нет	-	да	да	-
2	Windows Agent 2000/XP	-	нет	нет	-	нет	да	-
3	Linux	-	да	да\нет	-	да	да	-
4	AIX	-	нет	нет	-	нет	да	-
5	HP-UX	-	нет	нет	-	нет	да	-
6	Alt Linux	-	нет	нет	-	да	да	-
7	Astra Linux	-	да\нет	да\нет	-	да	да	-
8	Debian	-	да\нет	да\нет	-	да	да	-
9	FreeBSD	-	нет	нет	-	нет	да	-
10	Red OS	-	да\нет	да\нет	-	да	да	-
11	SunOS	-	нет	нет	-	нет	да	-
12	XenServer	-	нет	нет	-	нет	да	-
13	Active Directory Domain	-	нет	нет	-	нет	да	-
Виртуализация								

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
1	vCenter VCSA	-	нет	нет	-	нет	нет	нет
2	vCenter Windows	-	нет	нет	-	нет	нет	нет
3	Host	-	нет	нет	-	нет	нет	-
4	Host с контролем целостности по SSH	-	нет	нет	-	нет	нет	-
5	Host с контролем целостности по HTTPS	-	нет	нет	-	нет	нет	-
6	ESXi ОС с контролем целостности по SSH	-	да	да	-	да	да	да
7	ESXi ОС с контролем целостности по HTTPS	-	нет	нет	-	нет	нет	нет
8	Standalone ESXi с контролем целостности по SSH	-	нет	нет	-	нет	нет	нет
9	Standalone ESXi с контролем целостности по HTTPS	-	нет	нет	-	нет	нет	нет
10	VM	-	нет	нет	-	нет	нет	-
11	Virtual Machine Manager	-	нет	нет	-	нет	нет	-
12	Hyper-V хост	-	нет	нет	-	нет	нет	-
13	Hyper-V хост с контролем целостности	-	нет	нет	-	нет	нет	-
14	Standalone Hyper-v	-	нет	нет	-	нет	нет	-
15	Hyper-v VM	-	нет	нет	-	нет	нет	-
16	KVM	-	нет	нет	-	нет	да	-
17	zVirt	-	нет	нет	-	да	да	-
18	zVirt Host	-	нет	нет	-	нет	да	-
19	zVirt Host с контролем целостности по SSH	-	нет	нет	-	да	да	-
20	zVirt Vm	-	нет	нет	-	нет	да	-

№	Поддерживаемое оборудование	Лицензии						
		Efros NAC	Efros NA	Efros FA	Efros CM	Efros VC	Efros ICC	Efros NFA
21	Proxmox	-	нет	нет	-	нет	да	-
22	Proxmox Хост	-	нет	нет	-	нет	да	-
23	Proxmox Хост с контролем целостности по SSH	-	нет	нет	-	нет	да	-
24	Proxmox виртуальная машина	-	нет	нет	-	нет	да	-
25	Proxmox контейнер	-	нет	нет	-	нет	да	-
26	Скала-Р	-	нет	нет	-	нет	да	-
27	Скала-Р Виртуальная среда	-	нет	нет	-	нет	да	-
28	Скала-Р Хост	-	нет	нет	-	нет	да	-
29	Скала-Р Хост с контролем целостности по SSH	-	нет	нет	-	нет	да	-
30	Docker	-	нет	нет	-	да	да	-
31	Kubernetes	-	нет	нет	-	да	да	-
32	РЕД виртуализация	-	-	-	-	-	да	-
Прикладное программное обеспечение								
1	Firebird	-	-	-	-	нет	да	-
2	Jatoba	-	-	-	-	нет	да	-
3	Microsoft SQL	-	-	-	-	нет	да	-
4	MySQL	-	-	-	-	нет	да	-
5	Oracle	-	-	-	-	нет	да	-
6	PostgreSQL	-	-	-	-	да	да	-
7	Primo RPA Orchestrator	-	-	-	-	-	да	-
8	UiPath	-	-	-	-	нет	да	-
9	SCADA	-	-	-	-	нет	да	-

Примечание:

- да – поддерживается;
- нет – не поддерживается;
- да\нет – частично поддерживается;
- "–" – неприменимо для данного типа лицензии.