ГАЗИНФОРМ СЕРВИС

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

Модель лицензирования

Санкт-Петербург, 2024

Аннотация

Данный документ представляет собой описание модели лицензирования функциональных модулей программного комплекса по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO» или комплекс). Документ содержит сведения о возможностях функциональных модулей ПК «Efros DO», об основных положениях лицензирования, о лицензировании оборудования функциональных модулей, об условиях окончании срока лицензии комплекса.

Содержание

1 Основные сведения о ПК «Efros DO»

1.1 Расшифровка названий и краткое описание видов лицензий функциональных модулей ПК «Efros DO» приведены в таблице 1.

Таблица 1 – Расшифровка названия лицензии и краткое описание

Лицензия функционального модуля		**Описание**
Полное название	**Сокращенное название**	
NETWORK ASSURANCE	NA	Модуль контроля конфигураций и топологии сети
FIREWALL ASSURANCE	FA	Модуль оптимизации и настройки межсетевых экранов (МЭ)
CHANGE MANAGER	CM	Модуль анализа и управления объектами защиты в разделе «Центр задач»
VULNERABILITY CONTROL	VC	Модуль анализа уязвимостей и построения векторов атак
NETWORK FLOW ANALYSIS	NFA	Модуль сбора статистики по потокам данных в сети
INTEGRITY CHECK COMPLIANCE	ICC	Модуль контроля целостности и проверки соответствия хостов и конечных точек
NETWORK ACCESS CONTROL	NAC	Модуль разграничения и контроля доступа в сеть
SECURE DNS	SDNS	Модуль защиты DNS

1.2 Функциональные модули ПК «Efros DO» реализуют следующие функциональные возможности:

1) Функциональный модуль «Efros Network Assurance» (модуль «Efros NA»):
   - контроль изменения конфигураций сетевого оборудования;
   - контроль изменения конфигураций МЭ;
   - проверка соответствия безопасности сетевого оборудования;
   - проверка соответствия безопасности МЭ;
   - моделирование трафика на основе маршрутов и правил МЭ.

2) Функциональный модуль «Efros Firewall Assurance» (модуль «Efros FA»):
   - 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.
3) Функциональный модуль «Efros Integrity Check Compliance» (модуль «Efros ICC»):
   - контроль изменения конфигураций операционной системы (ОС), прикладного программного обеспечения (ППО), виртуализации, контейнеров и средств оркестрации;
   - контроль целостности файлов ОС, ППО, виртуализации, контейнеров и средств оркестрации;
   - проверки соответствия безопасности ОС, ППО, виртуализации, контейнеров и средств оркестрации.
4) Функциональный модуль «Efros Vulnerability Control» (модуль «Efros VC»):
   - выявление известных уязвимостей на основе версии ОС;
   - синхронизация списков уязвимостей с собственной базой данных по уязвимостям;
   - синхронизация с активными сканерами уязвимостей для получения информации об объекте защиты (ОЗ);
   - построение векторов атак.
5) Функциональный модуль «Efros Network Flow Analysis» (модуль «Efros «NFA»):
   - предоставление информации по соединениям с параметрами скорости, длительности и принадлежности к адресам;
   - сбор статистики использования сетевого трафика по соединениям и анализ активности;
   - работа с протоколами NetFlow, sFlow, IPFIX и NetStream.
6) Функциональный модуль «Efros Network Access Control» (модуль «Efros NAC»):
   - управление доступом в сетевые сегменты с применением расширенных политик доступа в сеть, управление административным доступом к активному сетевому оборудованию (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 ACO и списка сетевых устройств/конечных точек).

7) Функциональный модуль «Efros Change Manager» (модуль «Efros CM») реализует возможность автоматизации управления жизненным циклом правил МЭ.

8) Функциональный модуль «Efros Secure DNS» (модуль «Efros SDNS»):

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

2 Основные положения лицензирования

2.1 Возможности определенного функционального модуля ПК «Efros DO» доступны только при наличии лицензии на его использование.

2.2 Ключ лицензии активируется для всего комплекса в целом, в нем определены:

- перечень функциональных модулей;
- лимит количества доступных лицензий на оборудование для каждого из функциональных модулей;
- дата окончания действия лицензии комплекса;
- дата окончания технической поддержки.

2.3 Каждая лицензия на функциональный модуль (кроме «Efros SDNS») имеет определенное количество доступных лицензий на оборудование.

2.4 При достижении лимита по количеству лицензий на оборудование добавление нового оборудования или назначение новых функции невозможно. Для того чтобы добавить новое оборудование, необходимо удалить ранее добавленное оборудование или назначенные функции либо приобрести дополнительную лицензию.

3 Лицензирование оборудования модуля «Efros NA»

3.1 Функциональный модуль «Efros NA» обеспечивает контроль конфигураций и топологии сети для ОЗ с возможностью «Контроль устройств».

3.2 Подсчет лицензий оборудования происходит по количеству ОЗ с включенным типом контроля «NETWORK ASSURANCE».

3.3 Количество лицензий оборудования НЕ уменьшается в следующих случаях:

- для существующего ОЗ тип контроля «NETWORK ASSURANCE» выключен;
- выбранный тип устройства не лицензируется – не имеет ограничения по лицензированию (подробнее см. в документе «Описание применения»).

3.4 Количество лицензий оборудования увеличивается в следующих случаях:

- при выключении данного типа контроля для ОЗ;
- при удалении возможности «Контроль устройств» для ОЗ;
- при удалении ОЗ с возможностью «Контроль устройств».

4 Лицензирование оборудования модуля «Efros FA»

4.1 Функциональный модуль «Efros FA» обеспечивает возможности оптимизации и настройки межсетевых экранов.

4.2 Подсчет лицензий оборудования происходит по количеству ОЗ с назначенной возможностью «Контроль устройств».

4.3 Количество лицензий оборудования НЕ уменьшается в следующих случаях:

- для существующего ОЗ возможность «Контроль устройств» не назначена;
- выбранный тип устройства не лицензируется – не имеет ограничения по лицензированию (подробнее см. в документе «Описание применения»).

4.4 Количество лицензий оборудования увеличивается в следующих случаях:

- при удалении возможности «Контроль устройств» для ОЗ;
- при удалении ОЗ с возможностью «Контроль устройств».

5 Лицензирование оборудования модуля «Efros CM»

5.1 Функциональный модуль «Efros CM» предоставляет возможности анализа и управления объектами защиты в разделе «Центр задач».

5.2 Подсчет лицензий оборудования происходит по количеству ОЗ с назначенной возможностью «Контроль устройств».

5.3 Количество лицензий оборудования НЕ уменьшается в следующих случаях:

- для существующего ОЗ возможность «Контроль устройств» не назначена;
- выбранный тип устройства не лицензируется – не имеет ограничения по лицензированию (подробнее см. в документе «Описание применения»).

5.4 Количество лицензий оборудования увеличивается в следующих случаях:

- при удалении возможности «Контроль устройств» для ОЗ;
- при удалении ОЗ с возможностью «Контроль устройств».

6 Лицензирование оборудования модуля «Efros VC»

6.1 Функциональный модуль «Efros VC» обеспечивает анализ уязвимостей и построение векторов атак для ОЗ с возможностью «Контроль устройств».

6.2 Подсчет лицензий оборудования происходит по количеству ОЗ с включенным типом контроля «VULNERABILITY CONTROL».

6.3 Количество лицензий оборудования НЕ уменьшается в следующих случаях:

- для существующего ОЗ тип контроля «VULNERABILITY CONTROL» выключен;
- выбранный тип устройства не лицензируется – не имеет ограничения по лицензированию (подробнее см. в документе «Описание применения»).

6.4 Количество лицензий оборудования увеличивается в следующих случаях:

- при выключении данного типа контроля для ОЗ;
- при удалении возможности «Контроль устройств» для ОЗ;
- при удалении ОЗ с возможностью «Контроль устройств».

7 Лицензирование оборудования модуля «Efros NFA»

7.1 Функциональный модуль «Efros NFA» обеспечивает сбор статистики по потокам данных в сети.

7.2 Подсчет лицензий оборудования происходит по количеству уникальных IP-адресов, с которых поступает информация по трафику.

7.3 Количество лицензий оборудования уменьшается при назначении источника трафика.

7.4 Количество лицензий оборудования увеличивается при удалении источника трафика.

7.5 Количество триггеров[1] не ограничивается.

[1] Триггеры – индикаторы отклонения от заданной нормы параметров контролируемой сети

8 Лицензирование оборудования модуля «Efros ICC»

8.1 Функциональный модуль «Efros ICC» обеспечивает контроль целостности и проверку соответствия:

- ОС и ППО;
- систем управления базами данных (СУБД);
- виртуализации;
- контейнеров и средств оркестрации.

8.2 Комплекс автоматически определяет тип оборудования при включении контроля «INTEGRITY CHECK COMPLIANCE».

8.3 Подсчет лицензий оборудования происходит по количеству ОЗ с включенным типом контроля «INTEGRITY CHECK COMPLIANCE».

8.4 При назначении ОЗ возможности одновременно нескольких типов оборудования модуля «Efros ICC» (например, операционные системы и СУБД), значение количества лицензий оборудования уменьшается для каждого типа оборудования.

8.5 Количество лицензий оборудования НЕ уменьшается в следующих случаях:

- для существующего ОЗ тип контроля «INTEGRITY CHECK COMPLIANCE» выключен;
- выбранный тип устройства не лицензируется – не имеет ограничения по лицензированию (подробнее см. в документе «Описание применения»);
- подключение серверов управления средой виртуализации и виртуальных машин.

8.6 Количество лицензий оборудования увеличивается в следующих случаях:

- при выключении данного типа контроля для ОЗ;
- при удалении возможности «Контроль устройств» для ОЗ;
- при удалении ОЗ с возможностью «Контроль устройств».

9 Лицензирование оборудования модуля «Efros NAC»

9.1 Функциональный модуль «Efros NAC» обеспечивает разграничение и контроль доступа в сети для трех видов подключений:

- сетевое оборудование;
- активные сессии доступа в сеть;
- активные сессии доступа на оборудование.

9.2 Подсчет лицензий оборудования происходит по количеству одновременно активных сеансов.

9.3 При неактивности сетевого оборудования в течение определенного периода происходит автоматическое прерывание сессии доступа. Данный период устанавливается параметром «Длительность активной сессии» в ПК «Efros DO» (по умолчанию 5 дней).

9.4 Количество лицензий оборудования уменьшается в следующих случаях:

- при добавлении сетевого оборудования с возможностью «Контроль доступа»;
- при подключении активных сессий доступа в сеть:
  - IP-адрес – выделяется одна лицензия;
  - диапазон IP-адресов – выделяется несколько лицензий в соответствии с количеством IP-адресов в диапазоне;
- при подключении активных сессий доступа на оборудование:
  - IP-адрес – выделяется одна лицензия;
  - диапазон IP-адресов – выделяется несколько лицензий в соответствии с количеством IP-адресов в диапазоне.

9.5 Количество лицензий оборудования увеличивается в следующих случаях:

- при удалении сетевого оборудования с возможностью «Контроль доступа»;
- при завершении сессии доступа в сеть;
- при завершении сессии доступа на оборудование;
- при прерывании сессии доступа из-за неактивности (см. 9.3);
- при удалении ОЗ с возможностью «Контроль доступа».

10 Лицензирование модуля «Efros SDNS»

10.1 Функциональный модуль «Efros SDNS» обеспечивает возможность защиты DNS-трафика.

10.2 При наличии лицензии на функциональный модуль «Efros SDNS» доступно назначение следующих функций:

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

10.3 Подсчет лицензий оборудования не производится.

11 Окончание срока лицензии комплекса

11.1 По окончании срока действия лицензии пользователи комплекса блокируются. За 14 дней до даты окончания срока действия пользователи получают предупреждение в виде сообщения.

11.2 Все сервисы комплекса по сбору и логированию информации выполняют свою работу в течение 7 дней после окончания срока действия лицензии. Если в этот период лицензия будет продлена, работа комплекса не останавливается. Полная остановка работы комплекса происходит спустя 7 дней с даты окончания действия лицензии.

Перечень сокращений

CM	–	Change Manager
DNS	–	Domain Name System
FA	–	Firewall Assurance
ICC	–	Integrity Check Compliance
IP	–	Internet Protocol
LDAP	–	Lightweight Directory Access Protocol
MAC	–	Media Access Control
NA	–	Network Assurance
NAC	–	Network Access Control
NFA	–	Network Flow Analysis
RADIUS	–	Remote Authentication in Dial–In User Service
TACACS+	–	Terminal Access Controller Access Control System plus
VC	–	Vulnerability Control
АСО	–	Активное сетевое оборудование
МЭ	–	Межсетевой экран
ОЗ	–	Объект защиты
ОС	–	Операционная система
ПК	–	Программный комплекс
ППО	–	Прикладное программное обеспечение
СУБД	–	Система управления базами данных