Автономная некоммерческая организация дополнительного профессионального образования «Диона Мастер Лаб»

“УТВЕРЖДАЮ”

Директор И.Э. Левен

«07» апреля 2021 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«FG-SC: FortiGate Безопасность» (FortiGate Security)

г. Москва

2021 год

Содержание

1. Описание образовательной программы

Программа разработана в соответствии с приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам".

Повышение квалификации слушателей, осуществляемое в соответствии с программой, проводится с использованием модульного принципа построения учебного плана с применением различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения в соответствии с законодательством об образовании.

Дополнительная профессиональная программа повышения квалификации, разработана образовательной организацией в соответствии с законодательством Российской Федерации, включает все модули, указанные в учебном плане.

Содержание оценочных и методических материалов определяется образовательной организацией самостоятельно с учетом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. № 499.

Объем дополнительной профессиональной программы вне зависимости от применяемых образовательных технологий, должен быть не менее 16 академических часов. Сроки ее освоения определяются образовательной организацией самостоятельно.

Формы обучения слушателей (очная, очно-заочная, заочная) определяются образовательной организацией самостоятельно.

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;

- лица, получающие среднее профессиональное и (или) высшее образование.

Данная образовательная программа предназначена для:

- инженеров;
- системных администраторов;
- опытных ИТ-специалистов, работающих с продуктами Fortinet;
- администраторов, инженеров и архитекторов, которым необходимо планировать, внедрять или управлять окружением Fortinet
- специалистов в области сетевых технологий и информационной безопасности, занимающимся разработкой, внедрением и администрированием инфраструктуры сетевой безопасности, а именно обеспечением требуемого режима работы сетевых устройств, входящих в состав информационно-коммуникационных систем.

Образовательная деятельность слушателей предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, лабораторные работы, тренинги, консультации, выполнение аттестационной, дипломной, проектной работы и другие виды учебных занятий и учебных работ, определенные учебным планом.

Аннотация к образовательной программе

В рамках 3-дневного курса будут изучены дополнительные возможности настройки сетевых параметров и безопасности устройства FortiGate UTM. Во время прохождения обучения слушатели будут учиться настраивать маршрутизацию, работу в прозрачном режиме, познакомятся с инфраструктурой отказоустойчивости, изучат углубленные настройки IPsec VPN, работу web-прокси, диагностику и тонкую настройку производительности.

Курс рекомендован и будет полезен профессионалам в области сетевых технологий и информационной безопасности, занимающимся разработкой, внедрением и администрированием инфраструктуры сетевой безопасности FortiGate UTM. Данный курс является отправным в изучении основ работы с устройством FortiGate. По окончании курса полученные знания и навыки будут подтверждены Удостоверением о повышении квалификации.

2. Цели программы

Освоение функций и возможностей сервера шлюза FortiGate фирмы Fortinet. Обеспечение теоретических знаний и практических навыков, необходимых для внедрения и администрирования инфраструктуры сетевой безопасности FortiGate UTM. Данный курс подразумевает знание основ работы с устройством FortiGate.

3. Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональным стандартом «Системный администратор информационно-коммуникационных систем» (Код профессиональной деятельности 06.026 «Системный администратор информационно-коммуникационных систем»), утвержденным Приказом Минтруда России № 684н от 05.10.2015.

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанного вида профессиональной деятельности:

- Обеспечение требуемого режима работы сетевых устройств, входящих в состав инфокоммуникационной системы;
- Настройка сетевых элементов инфокоммуникационной системы;

Лица, успешно освоившие программу, должны овладеть следующими компетенциями:

Совершенствуемые компетенции

№№	Компетенция	**Направление подготовки** ФГОС ВО ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 09.02.06 «Сетевое и системное администрирование» / **Код компетенции**
1.	Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.	ПК 1.2.
2.	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.	ПК 1.3.
3.	Администрировать сетевые ресурсы в информационных системах.	ПК 2.2.
4.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	ПК 3.1.
5.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.	ПК 3.3.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта «Системный администратор информационно-коммуникационных систем» (Код профессиональной деятельности 06.026 «Системный администратор информационно-коммуникационных систем»), утверждённым Приказом Минтруда России от 05.10.2015 № 684н.

№№	Компетенция (наименование обобщённой трудовой функции)	Направление подготовки ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ стандарта 06.026 «Системный администратор информационно-коммуникационных систем», утверждённым Приказом Минтруда России от 05.10.2015 № 684н Наименование вида ПД: «Администрирование информационно-коммуникационных (инфокоммуникационных) систем»	
		Трудовые функции	
		Наименование	Код
D	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Настройка сетевых элементов инфокоммуникационной системы	D/01.6
		Управление безопасностью сетевых устройств и программного обеспечения	D/03.6
		Диагностика отказов и ошибок сетевых устройств и программного обеспечения	D/04.6
		Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	D/06.6
		Настройка систем резервного копирования и восстановления баз данных	E/03.7

После окончания обучения Слушатель будет знать:

- Основные возможности Fortinet UTM
- Идеологию построения и развёртывания Security Fabric
- Политики безопасности
- Трансляцию адресов и портов (NAT и PAT)
- Основы построения VPN, отличия SSL и IPSec VPN
- Методы и способы настройки и управления учетными записями пользователей и аутентификацией

После окончания обучения Слушатель будет уметь:

- Настраивать устройства FortiGate UTM
- Настраивать политику безопасности
- Строить защищённый канал передачи данных через Интернет
- Настраивать Антивирус
- Фильтровать Web-трафик
- Настраивать учётные записи Пользователей

Категория слушателей:

системные администраторы, системные инженеры, менеджеры по безопасности, сетевые инженеры, лица, готовящиеся к сдаче экзамен на сертификат “NSE 4 Network Security Professional”.

Требования к предварительной подготовке:

Наличие базового знания сетевых технологий, умения работать с Windows Server и UNIX, понимания TCP/IP и умения работать в Интернете.

4. Учебный план

Срок обучения: 24 академических часа, в том числе 24 аудиторных.

Самостоятельные занятия: не предусмотрены.

Форма обучения: очная, очно-заочная, заочная формы обучения, в том числе, с применением дистанционных образовательных технологий и электронного обучения. По желанию слушателя форма обучения может быть изменена и/или дополнена.

Режим занятий: дневной, вечерний

№ п/п	Наименование разделов программы	Всего (акад. часов)	В том числе		Формы аттестации
			Теория	Практика	
1	Глава 1: Введение в Fortinet UTM	1	0,5	0,5	Опрос, практические занятия
2	Глава 2: Security Fabric	1	0,5	0,5	Опрос, практические занятия
3	Глава 3: Политики безопасности	2	1	1	Опрос, практические занятия
4	Глава 4: Трансляция адресов и портов (NAT and PAT)	2	1	1	Опрос, практические занятия
5	Глава 5: Аутентификация пользователей	2	1	1	Опрос, практические занятия
6	Глава 6: Логирование и мониторинг	2	1	1	Опрос, практические занятия
7	Глава 7: Работа с сертификатами	1	0,5	0,5	Опрос, практические занятия
8	Глава 8: Фильтрация Web-трафика	1	1	1	Опрос, практические занятия
9	Глава 9: Управление приложениями	1	1	1	Опрос, практические занятия
10	Глава 10: Настройка антивируса	2	1	1	Опрос, практические занятия
11	Глава 11: IPS (система предотвращения вторжений)	2,5	1	1,5	Опрос, практические занятия
12	Глава 12: SSL VPN	2,5	1	1,5	Опрос, практические занятия

13	Итоговая аттестация	1	1	0	Зачёт
	Всего	24	12,5	11,5	

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы в порядке, установленном Положением об организации образовательного процесса в АНО Дополнительного профессионального образования «Диона Мастер Лаб».

5. Календарный учебный график

Учебный год: круглогодичное обучение.

Продолжительность Программы: 16академических часов.

Форма организации образовательного процесса: очная, очно-заочная (вечерняя) и заочная формы обучения, в том числе, с применением дистанционных образовательных технологий и электронного обучения.

Сменность занятий (при очной форме обучения): I смена.

Количество учебных дней в неделю при очном обучении: 2 дня.

Начало учебных занятий: 10.00

Окончание учебных занятий: 17.30

Продолжительность урока: 45 минут (1 академический час).

Продолжительность перемен: 15 минут, перерыв на обед – 60 минут.

Расписание занятий для очных групп:

День недели	№ Урока	Время
Конкретный день недели согласовывается во время учебного процесса	1 – 3	10:00 – 11:30
	4 – 5	11:45 – 13:15
	6 – 8	14:15 – 15:45
	9 – 10	16:00 – 17:30

6. Рабочая программа учебных предметов

День 1

Глава 1: Введение в Fortinet UTM

- Обзор основных возможностей FortiGate
- Режимы работы
- Учётная запись администратора, разграничение прав и доступа
- Восстановление пароля администратора
- Резервное копирование и восстановление
- Обновление программного обеспечения

- Настройка встроенных серверов DNS и DHCP
- Лабораторная работа: Инсталляция и первоначальная настройка системы

Глава 2: Security Fabric

- Идеология построения Fortinet Security Fabric
- Развёртывание Fortinet Security Fabric
- Развитие Security Fabric дополнительными компонентами и функциями
- Рейтинги и топология
- Лабораторная работа: Развёртывание Security Fabric

Глава 3: Политики безопасности

- Соотнесение трафика с правилами по адресам, портам, пользователям, интерфейсам и зонам
- Настройка политик файервола
- Использование номеров правил и ID правил
- Идентификация использованных объектов
- Изменение порядка правил для корректной работы
- Использование поиска по политике для определения подходящего правила
- Лабораторные работы: Создание политики безопасности

Глава 4: Трансляция адресов и портов (NAT and PAT)

- Идеология трансляции адресов и портов
- Режимы работы трансляции адресов
- Настройка политики файервола для трансляции адресов источника и получателя (VIP)
- Настройка централизованной трансляции (central NAT)
- Поддержка сессий на 7 уровне (session helpers), использование SIP session helper для VoIP
- Интерпретация записей в таблице сессий
- Анализ вывода команды диагностики сессий, состояния TCP, UDP и ICMP сессий
- Использование логов для решения общих проблем с NAT, мониторинг сессий с NAT
- Рекомендации по настройке NAT
- Лабораторная работа: Трансляция адресов

Глава 5: Аутентификация пользователей

- Основы аутентификации, методы аутентификации, протоколы
- Использование внешних серверов аутентификации
- Описание методов активной и пассивной аутентификации
- Настройка локальной, удалённой и двухфакторной аутентификации
- Настройка внешних серверов аутентификации
- Настройка портала (Captive Portal), политик и дисклеймеров для аутентификации
- Мониторинг пользователей на файерволе
- Использование методик отладки и рекомендаций
- Лабораторная работа: Аутентификация пользователей

День 2

Глава 6: Логирование и мониторинг

- Основы логирования, типы и подтипы лог-записей, их структура и уровни
- Влияние логирования на производительность
- Опции локального логирования, настройка
- Выделение места на диске, мониторинг использования диска, действия при переполнении
- Возможности логирования на внешние устройства, настройка
- Настройка передачи логов, обеспечение надёжности и использование шифрации

- Настройка логирования, работа демона miglogd
- Поиск и просмотр логов из командной строки и графического интерфейса
- Использование FortiView
- Настройка предупреждений по почте и весовых параметров угроз
- Настройка резервного копирования логов, их выгрузки и загрузки
- Лабораторная работа: Настройка логирования

Глава 7: Работа с сертификатами

- Понятие доверенных и недоверенных сертификатов
- Установление SSL соединения между FortiGate и SSL сервером
- Настройка инспектирования SSL трафика, два варианта настройки
- Использование полной инспекцию, помехи и их преодоление
- Запрос сертификата, импорт CRL, резервное копирование и восстановление сертификатов
- Лабораторная работа: Использование сертификатов

Глава 8: Фильтрация Web-трафика

- Описание режимов проверки трафика в FortiOS
- Использование полной инспекции SSL
- Профили фильтрации web-трафика
- Работа с категориями
- Переопределение категорий, настройка пользовательских категорий
- Запрос рейтинга в FortiGuard, настройка квот
- Переопределение web-профайлов, настройка фильтрации поисковых запросов
- Фильтрация web-контента
- Фильтрация DNS
- Настройка профайлов инспекции SSL/SSH трафика, настройка исключений
- Прикрепление профайлов к политике, анализ логов
- Лабораторная работа: Фильтрация web-трафика

Глава 9: Управление приложениями

- Основы управления приложениями, определение типов приложений
- Сервисы управления приложениями в FortiGuard
- Сигнатуры приложений
- Настройка управления приложениями в режиме профайлов
- Настройка управления приложениями в режиме политик
- Использование управления приложениями для шейпинга трафика
- Активация логирования и мониторинга событий, связанных с управлением приложениями
- Использование FortiView для детального просмотра логов
- Рекомендации по настройке управления приложениями
- Отладка работы механизма управления приложениями
- Лабораторная работа: Управление приложениями

Глава 10: Настройка антивируса

- Использование сигнатур антивируса
- Режимы работы антивируса
- Использование FortiSandbox
- Различные наборы сигнатур FortiGuard
- Сравнение режимов сканирования, применение профайлов в в proxy и flow режимах
- Настройка профайлов и особенностей протоколов
- Логирование и мониторинг событий, связанных с работой антивируса, просмотр статистики
- Рекомендации по настройке антивируса
- Использование аппаратных акселераторов для антивирусного сканирования

- Отладка работы механизмов антивирусного сканирования
- Лабораторная работа: Настройка антивируса

День 3

Глава 11: IPS

- Управление обновлениями IPS через FortiGuard
- Настройка сенсоров IPS
- Применение IPS к трафику через файервол
- Обнаружение DOS-атак, настройка DOS-политики
- Обнаружение атак на Web-трафик, настройка WAF-профайлов
- Выбор методологии применения IPS
- Отладка работы системы IPS
- Лабораторная работа: Настройка IPS

Глава 12: SSL VPN

- Понятие VPN, отличие SSL и IPSec VPN
- Режимы работы SSL VPN
- Аутентификация пользователей в SSLVPN
- Настройка SSL VPN, порталы, необходимые политики, realms, персональные закладки
- Проверка настроек клиенткой машины при подключении
- Использование двухфакторной аутентификации, ограничение доступа по IP и MAC адресу
- Логирование и мониторинг SSL VPN подключений, настройка таймеров
- Отладка работы SSL VPN
- Лабораторная работа: SSL VPN

7. Организационно-педагогические условия реализации Программы

Эффективному освоению программы призвана способствовать система организационно-педагогических условий её реализации:

- организация обучения как целостного педагогического процесса;
- проектирование содержания учебного материала на основе компетентностного подхода;
- высокий удельный вес используемых обучающих технологий деятельностного типа, активных видов учебных занятий и учебных работ;
- использование оценочных материалов, определяющих достижение планируемых результатов обучения;
- разработка учебно-методической и информационной составляющей программы (учебно-методические материалы: учебники, лабораторные практикумы, бесплатные WEB-ресурсы всемирной паутины (отечественные и зарубежные), тематические блоги, информационные каналы и страницы социальных сетей профильной тематики программы);
- наличие материально-технических условий (аудитории, средства обучения, современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий);
- учебные материалы по Программе включают: рабочую программу, раздаточные материалы по курсу, методические материалы по курсу, данные примеров по курсу. Учебное пособие по Программе выдаётся слушателям в бумажном или электронном виде в зависимости от формы обучения;

- наличие кадровых условий (обеспечение реализации программы педагогическими работниками, квалификация которых не только соответствует требованиям законодательства в сфере образования, но и отвечает высшим мировым стандартам) (актуальные профессиональные и экспертные экзамены общемировых сертификационных центров)).

8. Формы аттестации и оценочные материалы

Освоение Программы сопровождается промежуточной аттестацией обучающихся в формах, определённых учебным планом, и в порядке, установленном Положением об организации образовательного процесса в АНО ДПО «Диона Мастер Лаб».

Освоение Программы завершается итоговой аттестацией обучающихся в форме, определённой учебным планом, и в порядке, установленном Положением об организации образовательного процесса в АНО ДПО «Диона Мастер Лаб».

Конкретные формы и процедуры текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации слушателей устанавливаются образовательной организацией самостоятельно.

Текущий контроль включает в себя посещение семинаров, выполнение практических и лабораторных заданий (если предусмотрено).

Слушателям, успешно освоившим соответствующую Программу и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации на бланке, образец которого самостоятельно устанавливается организацией.

Слушателям, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из организации, выдаётся справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому организацией.

Оценочные материалы для промежуточной аттестации по Программе разрабатываются в форме лабораторных работ и/или контрольных вопросов после изучения каждого модуля.

Оценочные материалы для итоговой аттестации по Программе разрабатываются в форме теста.

9. Оценочные материалы к итоговой аттестации

Итоговая аттестация проводится в форме выполнения теста-задания. Результаты итоговой аттестации слушателей выставляются по двух бальной шкале («зачёт» / «незачёт»).

Итоговая аттестация считается пройденной («зачёт»), если слушатель выполнил все лабораторные работы и итоговое задание (не менее 60% правильных ответов).

1. **Вопрос**: Как поведёт себя FortiGate, если трафик на подпадает под действие на одного из правил Central SNAT?

   Варианты ответов:

   a. Транслирует пакеты с применением адреса интерфейса
   b. Пропустит сессию без применения трансляции
   c. Отбросит пакет молча
   d. Отбросит пакет с уведомлением отправителя

   Правильный ответ B

2. **Вопрос**: В каком режиме должен работать FortiGate, чтобы маршрутизировать трафик?

   Варианты ответов

   a. В прозрачном режиме
   b. В NAT режиме

   Правильный ответ B

3. **Вопрос**: Объек какого типа обязательно должен присутствовать в поле Source политики?

   Варианты ответов:

   a. User Group
   b. Local User Account
   c. Address
   d. Proxy Address

   Правильный ответ C

АНО ДПО "ДИОНА МАСТЕР ЛАБ"

Подписано цифровой подписью: АНО ДПО "ДИОНА МАСТЕР ЛАБ"
Дата: 2021.04.08 14:55:02 +03'00'