Автономная некоммерческая организация
дополнительного профессионального образования
«Диона Мастер Лаб»

“УТВЕРЖДАЮ”

Директор И.Э. Левен

_____

«____»_____2021 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«FG-FortiWeb: Fortinet: защита web-приложений (FortiWeb)

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 учётом положений законодательства об образовании Российской Федерации.

Структура дополнительной профессиональной программы соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утверждённого 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

Трёхдневный курс посвящён изучению развёртывания, настройке и решению проблем web application firewall (WAF) компании Fortinet - системы FortiWeb.

Курс включает изучение ключевых концепций безопасности веб-приложений и проведение лабораторных занятий, во время которых слушатели изучают функции защиты и обеспечения производительности. При выполнении лабораторных работ слушатели моделируют трафик и атаки с использованием реальных веб-приложений. Слушатели на практике изучают эффективное распределение нагрузки с виртуальных серверов на реальные, настраивая логические параметры, проверяя трафик и используя файлы cookies сеанса HTTP.

Курс предназначен для специалистов в области сетевых технологий и информационной безопасности, эксплуатирующих систему FortiWeb.

Курс является курсом подготовки к сдаче экзамена NSE6_FWB-6.1 - Fortinet NSE 6 - FortiWeb 6.1для получения уровня сертификации NSE 6.

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»), утверждённым Приказом Минтруда России № 684н от 05.10.2015.

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщённым 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

После окончания обучения Слушатель будет знать:

- угрозы уровня приложений
- как выбирать правильный режим работы
- как настраивать балансировку нагрузки для пула серверов
- применять SSL/TLS, аутентификацию и комплексный контроль доступа для незащищённых приложений
- как обучать FortiWeb для защиты заданных приложений
- как вносить в запретные списки подозреваемых в хакерстве, участии в DDoS-атаках и сборе данных

После окончания обучения Слушатель будет уметь:

- Противодействовать атакам типов defacement и DoS
- Предотвращать атаки "нулевого дня" без прерывания трафика
- Делать приложения соответствующими требованиям OWASP Top 10 for 2013 и PCI DSS 3.0
- Выявлять уязвимости серверов и web-приложений для надёжной и эффективной защиты
- Настраивать FortiGate и FortiWeb для усиления защиты приложений HTTP и XML
- Не допускать сканирование при работе FTP и SSH
- Настраивать блокирование и отчёты для внешних FortiADC / FortiGate и FortiAnalyze
- Решать проблемы с пропуском трафика, включая трафик FTP/SSH
- Диагностировать ошибочные срабатывания и настраивать сигнатуры
- Оптимизировать производительность

Категория слушателей:

системные администраторы, системные инженеры, менеджеры по безопасности, сетевые инженеры, лица, готовящиеся к сдаче экзамен NSE6_FWB-6.1 - Fortinet NSE 6 - FortiWeb 6.1 для получения уровня сертификации NSE 6.

Требования к предварительной подготовке:

Успешное изучение материала курсов FortiGate: Безопасность и Инфраструктура FortiGate
Знание модели OSI и протокола HTTP, Базовые знания HTML, JavaScript и PHP

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	1	0,5	0,5	Опрос, практические занятия
2	Глава 2. Базовые настройки	3	2	1	Опрос, практические занятия
3	Глава 3. Интеграция Front-End SNAT и балансировщиков нагрузки	2	1	1	Опрос, практические занятия
4	Глава 4. Машинное обучение и детектирование ботов	2	1	1	Опрос, практические занятия
5	Глава 5. Сигнатуры и проверка структуры трафика	2	1	1	Опрос, практические занятия
6	Глава 6. DoS атаки и подмена содержимого сайтов	2	1	1	Опрос, практические занятия
7	Глава 7. SSL и TLS	2	1	1	Опрос, практические занятия
8	Глава 8. Аутентификация и контроль доступа	2	1	1	Опрос, практические занятия
9	Глава 9. Соответствие PCI DSS 3.0	2	1	1	Опрос, практические занятия

10	Глава 10. Кэширование и сжатие	2	1	1	Опрос, практические занятия
11	Глава 11. Перезапись и перенаправление	2	1	1	Опрос, практические занятия
12	Глава 12. Решение проблем	1	0,5	0,5	Опрос, практические занятия
13	Итоговая аттестация	1	1	0	Зачёт
	Всего	24	13	11	

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: 24 академических 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
- Введение. Обзор возможностей FortiWeb. Типы атак и варианты развертывания защиты. Интерфейсы управления
- Базовые настройки. Варианты топологии. Начальные настройки. Отказоустойчивая конфигурация. Пулы серверов, политики, защищаемые хосты. Обработка трафика. Логирование
- Интеграция Front-End SNAT и балансировщиков нагрузки. Настройка FortiWeb. Настройка Front-end устройств
- Машинное обучение и детектирование ботов. Общее представление о машинном обучении. Скрытые Марковские процессы. Детектирование аномалий. Детектирование ботов,

День 2
- Сигнатуры и проверка структуры трафика. Написание сигнатур и правил. Проверка приходящих пакетов — куки сессий, валидация заголовков и тела пакетов. Проверка форм. Проверка состояния сессии.
- DoS атаки и подмена содержимого сайтов. Обзор вариантов атак. Проверка состояния трафика 3-7 уровней. Защита от подмены содержимого сайтов.
- SSL и TLS. Основы HTTPS. Алгоритмы шифрации и ключи. Сертификаты. Перенаправление с HTTP на HTTPS
- Аутентификация и контроль доступа. Методы управления доступом. Аутентификация. Работа в режиме AD FS proxy. Отслеживание аутентификации пользователей. Атаки на аутентификацию.

День 3
- Соответствие PCI DSS 3.0. Обзор PCI DSS. Определение степени уязвимости приложений. Противостояние основным угрозам.
- Кэширование и сжатие.
- Перезапись и перенаправление. Перенаправление трафика. Формирование регулярных выражений и их использование. Маршрутизайия HTTP трафика
- Решение проблем. Уменьшение количества ложных срабатываний. Проблемы с шифрацией. Улучшение производительности. Сбор статистики и отслеживание потока трафика.

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 двухбалльной шкале («зачёт» / «незачёт»).

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

1. **Вопрос**: Какой режим работы FortiWeb обеспечивает наилучшую защиту?

   Варианты ответов:

   a. True transparent proxy
   b. Reverse proxy
   c. Offline mode
   d. WCCP mode

   Правильный ответ B

2. **Вопрос**: Что из перечисленного возможно в режиме SSL инспекции но НЕ в режиме SSL Offloading?

   Варианты ответов

   a. Возможность аутентификации сертификатами для пользователей
   b. Расположение FortiWeb offline

   Правильный ответ B

3. **Вопрос**: Какой тип передаваемых данных хорошо архивируется?

   Варианты ответов:

   a. Файлы в формате PDF
   b. Файлы в формате JPG
   c. Файлы .css
   d. HTML файлы на китайском языке

   Правильный ответ C