Автономная некоммерческая организация дополнительного профессионального образования «Диона Мастер Лаб»

УТВЕРЖДАЮ

Директор АНО ДПО «Диона Мастер Лаб»

_____ И.Э. Левен

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«PAN-210: Основы инсталляции, настройки и управления межсетевым экраном Palo Alto версии 10.x» (Palo Alto Networks Firewall 10.x Essentials: Configuration and Management)

г. Москва

2020 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 24 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 Palo Alto Networks;
- администраторов, инженеров и архитекторов, которым необходимо планировать, внедрять или управлять систем безопасности PAN
- 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.

PAN Gateway - шлюз безопасности, устанавливаемый на периметр сети и выполняющий функции межсетевого экрана, потокового антивируса, антибота, IPS и аналогичные им.

Palo Alto Networks Operation System (PAN-OS)– операционная система устройств информационной безопасности.

Курс обеспечивает слушателям глубокие теоретические знания и практические навыки по инсталляции, настройке и управлению всеми межсетевыми экранами из линейки Next-Generation компании Palo Alto Networks. Слушатели познакомятся с механизмами настройки безопасности, сетевого взаимодействия, предупреждения угроз, идентификации приложений, идентификации пользователей, построения VPN туннелей, логирования и построения отчетов операционной системы Palo Alto Networks Operation System

Курс рекомендован и будет полезен сетевым инженерам, персоналу технической поддержки и инженерам безопасности, работающим с оборудованием обеспечения безопасности под программным обеспечением Palo Alto.

По окончании курса полученные знания и навыки будут подтверждены Удостоверением о повышении квалификации.

2. Цели программы

Освоение функций и возможностей шлюза безопасности (Security Gateway) фирмы Palo Alto Networks. Обеспечение теоретических знаний и практических навыков, необходимых для настройки программных компонентов и повседневной работы с инфраструктурой информационной безопасности, построенной на основе решения PAN-OS 10.x.

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.

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.	Администрировать сетевые ресурсы в информационных системах.	ПК 2.2.
2.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	ПК 3.1.
3.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	ПК 3.2.
4.	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»), утвержденным Приказом Минтруда России от 05.10.2015 № 684н.

№№	Компетенция (наименование обобщенной трудовой функции)	Направление подготовки ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ стандарта 06.026 «Системный администратор информационно-коммуникационных систем», утвержденным Приказом Минтруда России от 05.10.2015 № 684н Наименование вида ПД: «Администрирование информационно-коммуникационных (инфокоммуникационных) систем»	
		Трудовые функции	
		Наименование	Код
C	Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации	Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	C/02.6
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
F	Администрирование системного программного обеспечения инфокоммуникационной системы организации	Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	F/05.7

После окончания обучения Слушатель будет знать:

- Методы и способы управления политиками безопасности
- Принципы и способы иерархического построения политики безопасности
- Программные компоненты и лицензирование
- Методы и способы мониторинга трафика и соединений
- Основы построения VPN
- Методы и способы настройки и управления учетными записями пользователей и аутентификацией

После окончания обучения Слушатель будет уметь:

- Производить первоначальную настройку устройства
- Настраивать интерфейсы межсетевого экрана
- Создавать и редактировать политику безопасности
- Настраивать адресную трансляцию
- Настраивать механизм фильтрации шифрованного трафика
- Конфигурировать фильтрацию контента
- Строить VPN туннели
- Мониторить состояние устройства и анализировать логи трафика
- Настраивать отказоустойчивый кластер

Категория слушателей:

Сетевые инженеры, персонал технической поддержки и инженеры безопасности, работающим с оборудованием обеспечения безопасности под программным обеспечением Palo Alto.

Требования к предварительной подготовке:

Данный курс предполагает наличие у слушателей базовых знаний сетевых технологий, включая основы маршрутизации, коммутации и формирования IP адресов. Слушатели также должны быть знакомы с концепцией обеспечения безопасности с помощью пакетных фильтров. Приветствуются углубленные знания в области компьютерной безопасности — IPS, content filtering, proxy.

4. Учебный план

Срок обучения: 40 академических часов, в том числе 40 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	**Модуль 0: Введение** **Модуль 1: Обзор платформ и архитектуры**	1	1	0	Опрос
2	**Модуль 2: Подключение устройства к сети управления**	1,5	1	0,5	Опрос, практические занятия
3	**Модуль 3: Настройка конфигурации**	2	1	1	Опрос, практические занятия
4	**Модуль 4: Учетные записи администраторов**	2	1	1	Опрос, практические занятия
5	**Модуль 5: Подключение к рабочей сети**	1,5	0,5	1	Опрос, практические занятия
	День 2				
6	**Модуль 6: Жизненный цикл кибератак**	2	1	1	Опрос, практические занятия
7	**Модуль 7: Политики безопасности и адресной трансляции**	2	1	1	Опрос, практические занятия
8	**Модуль 8: Блокирование атак 3-4 уровней**	2	1	1	Опрос, практические занятия

9	**Модуль 9: Использование черных списков для защиты от атак**	2	1	1	Опрос, практические занятия
	День 3				
10	**Модуль 10: Идентификация приложений (App-ID)**	2	1	1	Опрос, практические занятия
11	**Модуль 11: Работа с политиками на основе идентификации приложений**	2	1	1	Опрос, практические занятия
12	**Модуль 12: Создание собственных приложений**	2	1	1	Опрос, практические занятия
13	**Модуль 13: Идентификация пользователей**	2	1	1	Опрос, практические занятия
	День 4				
14	**Модуль 14: Идентификация устройств**	2	1	1	Опрос, практические занятия
15	**Модуль 15: Блокирование неизвестных атак**	2	1	1	Опрос, практические занятия
16	**Модуль 16: Блокирование атак в шифрованном трафике**	2	1	1	Опрос, практические занятия
17	**Модуль 17: Предотвращение использования украденных учетных данных**	2	1	1	Опрос, практические занятия
	День 5				
18	**Модуль 18: Идентификация контента (Content-ID)**	2	1	1	Опрос, практические занятия
19	**Модуль 19: Мониторинг и построение отчетов**	2	1	1	Опрос, практические занятия
20	**Модуль 20: Что дальше**	3	0,5	2,5	Опрос, практические занятия
21	Итоговая аттестация	1	1	0	Зачет
	Всего	**40**	**20**	**20**	

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: Ошибка! Источник ссылки не найден.0 академических асов.

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: Ошибка! Источник ссылки не айден. 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 – 2	10:00 – 11:30
	3 – 4	11:45 – 13:15
	5 – 6	14:15 – 15:45
	7 – 8	16:00 – 17:30

6. Рабочая программа учебных предметов

День 1
Модуль 0: Введение

Модуль 1: Обзор платформ и архитектуры

- Обзор платформ безопасности
- Архитектура обеспечения проверки за один проход
- Аппаратные и виртуальные платформы

Модуль 2: Подключение устройства к сети управления

- Графическая среда управления, командная строка и API
- Первоначальный доступ к системе

- Настройка интерфейса управления
- Установка обновлений операционной системы и программ, лицензирование
- Лабораторная работа — Первоначальная настройка
-

Модуль 3: Настройка конфигурации

- Управление конфигурациями, текущая конфигурация и кандидат-конфигурация
- Работа с логами
- Лабораторная работа — Настройка конфигурации

Модуль 4: Учетные записи администраторов

- Аутентификация и авторизация в системе
- Создание локальных учетных записей администраторов
- Использование внешних серверов аутентификации
- Создание учетных записей для неинтерактивного входа
- Лабораторная работа — Работа с учетными записями администраторов

Модуль 5: Подключение к рабочей сети

- Использование сегментации сети для блокирования угроз
- Зоны (Security Zones) и интерфейсы
- Модель безопасности Zero Trust
- Типы интерфейсов — L2, L3, Virtual Wire, Tap, VLAN, loopback
- Сабинтерфейсы
- Виртуальные маршрутизаторы
- Лабораторная работа — Настройка зон и интерфейсов

День 2

Модуль 6: Жизненный цикл кибератак

Обзор жизненного цикла атак
- Типы атак
- Этапы прохождения трафика через файервол и предотвращение угроз

Модуль 7: Политики безопасности и адресной трансляции

- Базовые концепции политики безопасности
- Настройка и управление политикой безопасности
- Политика трансляции адресов
- Настройка трансляции адреса источника (Source NAT)
- Настройка трансляции адреса получателя (Destination NAT)
- Лабораторная работа — Политика безопасности и адресной трансляции

Модуль 8: Блокирование атак 3-4 уровней

- Блокирование атак с помощью профайлов защиты зон
- Блокирование атак с помощью политики защиты от DoS-атак
- Использование механизма защиты буферов пакетов
- Лабораторная работа — Защита от атак 3-4 уровней

Модуль 9: Использование черных списков для защиты от атак

- Блокирование доступа с IP адресов и на IP адреса из черного списка
- Блокирование доступа на и из доменов из черного списка
- Блокирование доступа на и с URL из черного списка
- Использование других механизмов URL-фильтрации
- Лабораторная работа — Применение черных списков для блокировки атак

День 3

Модуль 10: Идентификация приложений (App-ID)

- Процесс идентификации приложений
- Использование приложений в политике безопасности
- Идентификация неизвестных приложений
- Лабораторная работа — Основы идентификации приложений

Модуль 11: Работа с политиками на основе идентификации приложений

- Миграция с правил для портов на правила для приложений
- Поддержание политики в актуальном состоянии
- Обновление сигнатур приложений
- Лабораторная работа — Обслуживание политики на основе приложений

Модуль 12: Создание собственных приложений

- Варианты действий с неизвестными приложениями
- Перехват пакетов
- Определение уникальных сигнатур
- Создание собственных приложений
- Создание политик переопределения приложений
- Лабораторная работа — Блокирование атак с помощью собственных приложений

Модуль 13: Идентификация пользователей

- Обзор механизма идентификации пользователей
- Методы сопоставления пользователей с адресами
- Настройка идентификации пользователей
- Настройка встроенного агента идентификации
- Настройки агента идентификации под Windows
- Соотнесение пользователей с группами
- Создание динамических групп
- Использование учетных записей в политике безопасности
- Лабораторная работа — Идентификация пользователей

День 4

Модуль 14: Идентификация устройств

- Концепции идентификации устройств
- Настройка и лицензирование механизма идентификации устройств
- Поиск устройств и управление политиками

- Мониторинг устройств

Модуль 15: Блокирование неизвестных атак

- Концепции WildFire
- Настройка и управление WildFire
- Отчеты WildFire
- Лабораторная работа — WildFire

Модуль 16: Блокирование атак в шифрованном трафике

- Концепции расшифровки SSL
- Работа с сертификатами
- Расшифровка исходящего SSL трафика
- Расшифровка входящего SSL трафика
- Расшифровка SSH трафика
- Работа с мастер-ключом
- Дополнительные настройки — неподдерживаемые приложения, отказ от расшифровки, зеркалирование трафика, аппаратные модули, отладка и исправление неполадок
- Лабораторная работа — Расшифровка SSL трафика
-

Модуль 17: Предотвращение использования украденных учетных данных

- Использование мультифакторной аутентификации
- Предотвращение кражи учетных данных
- Лабораторная работа - Предотвращение использования украденных учетных данных

Модуль 18: Идентификация контента (Content-ID)

- Обзор механизмов идентификации контента
- Защита на основе сигнатур
- Реализация URL-фильтрации
- Блокирование передачи файлов
- Блокирование неизвестных угроз
- Блокирование трафика, содержащего запрещенные для передачи данные
- Использование идентификации контента в политике безопасности
- Лабораторная работа — Идентификация контента

День 5

Модуль 19: Мониторинг и построение отчетов

- Работа с закладками Dashboard, ACC и Monitor
- Перенаправление логов на внешние сервера
- Использование syslog
- Настройка SNMP
- Готовые шаблоны отчетов и создание собственных шаблонов
- Лабораторная работа — Мониторинг и построение отчетов

Модуль 20: Что дальше?

- Рекомендации по дальнейшему прохождению курсов для разных типов работ

- Рекомендации по подготовке к сдаче сертификационных экзаменов
- Лабораторная работа — Полная настройка системы

7. Организационно-педагогические условия реализации Программы

Эффективному освоению программы призвана способствовать система организационно-педагогических условий ее 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 выдается 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, определенных 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, определенной 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, выдается 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 («зачет» / «не зачет»).

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

1. **Вопрос**: Какие четыре модели из перечисленных существуют?

   Варианты ответов:

   a. PA-200
   b. PA-2000
   c. PS-300
   d. PA-3000
   e. PA-400
   f. PA-5000
   g. PA-7000

   Правильные ответы A, D, F,G

2. **Вопрос**: Существует специализированный интерфейс управления, обладающий следующими свойствами (выберите три)

   Варианты ответов:

   a. По умолчанию называется MGT
   b. Пропускает только управляющий трафик и не может быть настроен для транзита
   c. Используется для прямого подключения к плоскости управления
   d. Не может использовать DHCP

   Правильные ответы: A, B, C

3. **Вопрос**: Виртуальные маршрутизаторы поддерживают статическую маршрутизацию и следующие протоколы динамической маршрутизации (выберите три)?

   Варианты ответов:

   a. OSPF
   b. RIP
   c. EGRP
   d. BGP

   Правильные ответы: A, B, D

4. **Вопрос**: Какого из трех возможных типов будет вновь создаваемое правило?

   Варианты ответов:

   a. intrazone
   b. interzone
   c. universal

   Правильный ответ: C

5. **Вопрос**: Группа приложений может содержать приложения, фильтры и другие группы приложений, да или нет?

   Варианты ответов:

   a. да
   b. нет

   Правильный ответ: A

6. **Вопрос**: К какому объекту применяется Zone Protection Profile?

   Варианты ответов:
   a. Интерфейсы, на которые приходит трафик
   b. Правила политики безопасности
   c. Интерфейсы, с которых уходит трафик
   d. Группы адресов

   Правильный ответ: A