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

«CCSA-R80.X: Сертифицированный администратор Check Point R80.X»
(Check Point Certified Administrator R80.X)

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 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 Check Point Software Technologies;
- администраторов, инженеров и архитекторов, которым необходимо планировать, внедрять или управлять окружением Check Point R80.X
- 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

Трехдневный курс Check Point Security Administration является основой для изучения работы с сервером управления (Security Management) и шлюзом безопасности (Security Gateway) фирмы Check Point Software Technologies. Курс обеспечивает теоретические знания и практические навыки, необходимые для настройки программных блейдов (Software Blades), дает все необходимое для повседневной работы с инфраструктурой информационной безопасности, построенной на основе решения Check Point R80.40.

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

2. Цели программы

Изучение тонкости работы шлюзов безопасности, механизмов обновления, автоматизации и оркестрации, механизмов обеспечения отказоустойчивости, вариантов ускорения обработки трафика, особенностей аудита систем и построения отчетов, возможностей безопасного подключения удаленных пользователей, предотвращения «угроз нулевого дня», работы системы предотвращения вторжений и антивируса..

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.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	ПК 3.1.
2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	ПК 3.2.
3.	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
		Мониторинг событий, возникающих в процессе работы инфокоммуникационной системы	C/03.6
D	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Управление безопасностью сетевых устройств и программного обеспечения	D/03.6

После окончания обучения Слушатель будет знать:

- Способы углубленного управления системой
- Автоматизацию и оркестрацию, как выполнять настройку сервера Check Point API
- Способы и методы внедрения отказоустойчивости инфокоммуникационной системы
- Способы ускорения обработки трафика
- Архитектуру SmartEvent (коррелятор)
- Способы запуска, возможности и методы развертывания VPN удаленного доступа
- Техники глубокого анализа трафика

После окончания обучения Слушатель будет уметь:

- Корректно администрировать оборудование Check Point работающее на версии R80.40
- Отслеживать сетевую активность оборудования
- Писать политики, отвечающие за обработку трафика.
- Использовать оборудование для построения VPN
- Использовать различные методы аутентификации, для предоставления доступа на уровне учетных записей пользователей.

Категория слушателей:

системные администраторы, системные инженеры, менеджеры по безопасности, сетевые инженеры, лица, готовящиеся к сдаче экзамен на сертификат CCSA.

Требования к предварительной подготовке:

Данный курс предполагает наличие у слушателей базового знания сетевых технологий, умения работать с Windows Server и UNIX, понимания TCP/IP и умения работать в Интернете. Кроме того, рекомендуется опыт практической работы с продуктами Check Point от 6 месяцев до года.

4. Учебный план

Срок обучения: 24 академических часа, в том числе 12 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. Обзор технологии Check Point	1,5	1.5	0	Опрос, практические занятия
2	Глава 2. Варианты развертывания	2,5	1	1.5	Опрос, практические занятия
3	Глава 3. Компоненты Check Point и их взаимодействие	2,5	1,5	1	Опрос, практические занятия
4	Глава 4. Лицензирование	1,5	1	0.5	Опрос, практические занятия
5	Глава 5. Управление политиками безопасности	2,5	1,5	1	Опрос, практические занятия
6	Глава 6. Работа со слоями	2	1	1	Опрос, практические занятия
7	Глава 7. Управление доступом пользователей	2	1	1	Опрос, практические занятия
8	Глава 8. Трансляция адресов	1,5	0,5	1	Опрос, практические занятия
9	Глава 9. Работа с лог-записями	0,9	0,4	0.5	Опрос, практические занятия
10	Глава 10. Мониторинг состояния системы	0,9	0.4	0.5	Опрос, практические занятия
11	Глава 11. Использование SmartEvent	0,9	0.4	0.5	Опрос, практические занятия
12	Глава 12. Основные концепции VPN	2	1	1	Опрос, практические занятия
13	Глава 13. Работа с кластером	0,9	0.4	0.5	Опрос, практические занятия

14	Глава 14. Административные задачи	1,4	0,4	1.5	Опрос, практические занятия
15	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 часа.

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

Глава 1. Обзор технологии Check Point

- Архитектура централизованного управления, ее компоненты
- Типы межсетевых экранов, управление сетевым трафиком
- Архитектура шлюзов безопасности и варианты развертывания

Глава 2. Варианты развертывания

- Аппаратная и программная реализации
- Облачные решения, масштабируемые платформы
- Совместная и раздельная установка, прозрачный режим
- Основы операционной системны Gaia — интерфейс командной строки, пользователи, роли, монопольный доступ к настройкам, механизм апгрейда
- Лабораторная работа. Инсталляция сервера управления в режиме Primary
- Лабораторная работа. Инсталляция и настройка шлюза безопасности

Глава 3. Компоненты Check Point и их взаимодействие

- Механизм шифрованной передачи данных между модулями
- Утилита SmartConsole, инсталляция, компоненты интерфейса
- Дополнительные утилиты управления
- Учетные записи администраторов
- Сессии управления, сохранение версий базы настроек.
- Лабораторная работа. Установление шифрованного соединения
- Лабораторная работа. Учетные записи администраторов

Глава 4. Лицензирование

- Обзор лицензий, постоянные лицензии и подписки, центральные и локальные лицензии, активация лицензий, лицензирование аппаратных реализаций
- Работа с утилитой SmartUpdate
- Управление лицензиями, добавление, подключение и отключение, просмотр, экспорт, контракты, построение отчетов о состоянии лицензий
- Лабораторная работа. Управление лицензиями

Глава 5. Управление политиками безопасности

- Введение в политику безопасности, правила, объекты, зоны, антиспуфинг, Global Properties, секции
- Публикация изменений
- Policy Package, типы политик, унифицированная политика, общие политики
- Инсталляция политики
- Лабораторная работа. Создание объектов
- Лабораторная работа. Написание правил
- Лабораторная работа. Инсталляция политики

Глава 6. Работа со слоями

- Концепция слоя, слои политики управления доступом
- Упорядоченные и вложенные слои
- Лабораторная работа. Упорядоченные слои
- Лабораторная работа. Вложенные слои

Глава 7. Управление доступом пользователей

- Компоненты системы обеспечения доступа пользователей, выбор источника информации о пользователях
- Управление учетными записями пользователей, работа в SmartConsole и использование протокола LDAP
- Аутентификация пользователей
- Роли доступа
- Captive Portal
- Лабораторная работа. Обеспечение доступа пользователей

Глава 8. Трансляция адресов

- Режимы трансляции адресов, Hide и Static варианты
- Автоматически сформированные и написанные вручную правила
- Лабораторная работа. Настройка автоматического формирования правил трансляции

Глава 9. Работа с лог-записями

- Сбор информации
- Настройка логов
- Режимы просмотра
- Анализ логов
- Отслеживание работы правил
- Готовые выборки, язык формирования выборок
- Лабораторная работа. Генерация и анализ логов

Глава 10. Мониторинг состояния системы

- Система предупреждений в утилитах SmartConsole и SmartView Monitor
- Мониторинг подозрительной активности (SAM Rules)
- Мониторинг состояний шлюзов
- Списки пользователей и туннелей, системные счетчики, совместная работа, обзор трафика
- Лабораторная работа. Мониторинг состояния системы

Глава 11. Использование SmartEvent

- Обзор системы SamrtEvent, архитектура, компоненты
- Определение события
- Настройка реакции на события
- Построение отчетов, готовые и кастомизированные отчеты, анализ настроек безопасности
- Лабораторная работа. Построение отчетов

Глава 12. Основные концепции VPN

- Основы VPN, компоненты
- Развертывание VPN, Site-to-Site и Remote Access VPN
- VPN сообщества (Communities), их типы, взаимодействие
- Использование VPN сообществ в правилах
- Управление туннелями, постоянные туннели, тестирование и мониторинг туннелей
- Лабораторная работа. Построение простого варианта VPN

Глава 13. Работа с кластером

- Обзор технологии ClusterXL
- Развертывание кластера в режиме High Availability
- Обработка сбоев, инициирование сбоя вручную
- Синхронизация модулей
- Мониторинг состояния кластера
- Лабораторная работа. Работа с кластером

Глава 14. Административные задачи

- Настройка компонента Compliance, проверка соответствия настроек рекомендациям и стандартам, мониторинг
- Использование утилиты cpview
- Лабораторная работа. Тонкая настройка политики
- Лабораторная работа. Утилита cpview
- Лабораторная работа. Резервное копирование и восстановление

7. 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.

8. 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).

Пример материалов для итоговой аттестации.

1. **Вопрос**: Какой компонент продукта Smart Event отвечает за хранение events?

   Варианты ответов:

   a. Smart Event Client
   b. Smart Event Server
   c. Smart Event Correlation Unit

   Правильный ответ: B

2. **Вопрос**: В каком месте на шлюзе безопасности делается трансляция адреса источника сообщения?
   Варианты ответов:
   a. Трансляция адреса источника делается ближе к клиенту в операционной системе шлюза безопасности.
   b. Трансляция адреса источника делается ближе к серверу в операционной системе шлюза безопасности.
   c. Трансляция адреса источника делается ближе к серверу в ядре шлюза безопасности
   d. Шлюз безопасности не умеет выполнять данный тип трансляции.

   Правильный ответ: C

3. **Вопрос**: Какой порт используется в кластере для выполнения дельта синхронизации?
   Варианты ответов:
   a. UDP 8116
   b. TCP 256
   c. Полная синхронизация в кластере не выполняется , только дельта синхронизация
   d. HTTP 900

   Правильный ответ: A

4. **Вопрос**: Сколько администраторов одновременно может править один и тот же объект базы данных сервера управления в релизе R80?
   Правильный ответ: В релизе R80 один и тот же объект может править одновременно только один администратор.
5. **Вопрос**: Перечислите компоненты входящие в состав продукта Smart Event?

   Правильные ответы: Smart Event Server, Smart Event Correlation Unit, Smart Event Client.