НОЧУ ДПО УЦ «Сетевая Академия»

УТВЕРЖДАЮ
Директор НОЧУ ДПО УЦ «Сетевая Академия»
_____/Шикова Ю.В./

Образовательная программа
дополнительного профессионального образования
(повышения квалификации)
«Подготовительный курс к экзамену CompTIA Security+»
(Код- IS-6.0)

Содержание

Описание образовательной программы

Настоящая образовательная программа повышения квалификации (далее – Программа) разработана в соответствии с:

1. Федеральным законом от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»
2. Приказом Минобрнауки России от 1 июля 2013 г. N 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»
3. Уставом НОЧУ ДПО УЦ «Сетевая Академия»

Структура Программы включает цели, планируемые результаты обучения, учебный план, календарный учебный график, рабочую программу, организационно-педагогические условия, формы аттестации и оценочные материалы.

Цели Программы содержат описание целевой аудитории, целей обучения и необходимых начальных знаний и навыков слушателей.

Планируемые результаты обучения представлены в виде перечня профессиональных компетенций в рамках имеющейся квалификации (с отсылкой к профессиональному стандарту), качественное изменение которых осуществляется в результате обучения.

Учебный план определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

Календарный учебный график определяет основные параметры учебного процесса при организации занятий по освоению настоящей Программы, включая формы обучения, расписание занятий очных групп и т.п.

Рабочая программа раскрывает рекомендуемую последовательность изучения разделов (модулей).

Описание организационно-педагогических условий реализации Программы определяет организационные и методические требования НОЧУ ДПО УЦ «Сетевая Академия» к организации и проведению обучения по Программе.

Формы аттестации и оценочные материалы определяют формы проведения промежуточной и итоговой аттестации по Программе и форму учебно-методических материалов, необходимых для проведения указанных видов аттестации.

Цели программы

Данная Программа предназначена для:

- IT-специалистов, заинтересованных в получении минимального набора знаний и навыков по основам информационной безопасности и последующей сдачи сертификационного экзамена CompTIA Security+.

Целью обучения является приобретение знаний, соответствующих требованиям American National Standards Institute к минимальному набору знаний и навыков по основам ИБ

Для изучения данной Программы рекомендуется обладать следующими знаниями и навыками:

- Сертификация CompTIA A+, Network+ и Server+ или эквивалентный набор знаний и навыков.
- 2-летний опыт администрирования сети (Windows\Linux\Unix).

Планируемые результаты обучения

Реализация Программы направлена на повышение профессионального уровня в рамках имеющейся квалификации, определяемой профессиональным стандартом «06.032 Специалист по безопасности компьютерных систем и сетей.», утвержденным Приказом Минтруда России от 01.11.2016 № 598н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей".

Результатами обучения по Программе станут знания и умения, соответствующие следующим обобщенным трудовым функциям указанного профессионального стандарта:

- Обслуживание средств защиты информации в компьютерных системах и сетях.
- Администрирование средств защиты информации в компьютерных системах и сетях.

Совершенствуемые компетенции в соответствии с трудовыми функциями профессионального стандарта:

Компетенция	**Содержание компетенции** Трудовые функции	**Код**
Обслуживание средств защиты информации в компьютерных системах и сетях.	Обслуживание программно-аппаратных средств защиты информации в операционных системах	A/01.5
	Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях	A/02.5
	Обслуживание средств защиты информации прикладного и системного программного обеспечения	A/03.5
Администрирование средств защиты информации в компьютерных системах и сетях	Администрирование подсистем защиты информации в операционных системах	B/01.6
	Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6
	Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6

После обучения слушатель сможет:

- Сдать сертификационный экзамен CompTIA Security+.

Учебный план

Учебный план Программы определяет перечень, трудоемкость, последовательность и распределение модулей, иных видов учебной деятельности обучающихся и формы аттестации.

№ п/п	Наименование разделов (модулей)	Всего, час	В том числе		Форма аттестации
			Лекции	Практические занятия	
1.	Основы информационной безопасности	5	2,5	2,5	Опрос, практические занятия
2.	Угрозы и уязвимости	3	1,5	1,5	Опрос, практические занятия
3.	Управление безопасностью данных, приложений и хостов	3	1,5	1,5	Опрос, практические занятия
4.	Безопасность сети	4	2	2	Опрос, практические занятия
5.	Контроль доступа, аутентификация и управление учетными записями	3	1,5	1,5	Опрос, практические занятия
6.	Управление сертификатами	4	2	2	Опрос, практические занятия
7.	Соответствие требованиям и безопасность операций	3	1,5	1,5	Опрос, практические занятия
8.	Управление рисками	4	2	2	Опрос, практические занятия
9.	Управление инцидентами ИБ, поиск и устранение неисправностей	3	1,5	1,5	Опрос, практические занятия
10.	Обеспечение непрерывности бизнеса и планирование восстановления после катастроф	4	2	2	Опрос, практические занятия
11.	Знакомство с экзаменом.	2	1	1	Опрос, практические занятия
12.	Итоговая аттестация	2	-	2	Тестирование
	Итого:	**40**	**19**	**21**	

Допускается формирование индивидуального учебного плана для каждого слушателя в пределах осваиваемой Программы в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

Календарный учебный график

Учебный год: круглогодичное обучение.

Продолжительность Программы: 40 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: 5 дней.

Начало учебных занятий: 9.30

Окончание учебных занятий: 17.00

Продолжительность урока: 45 минут (1 академический час).

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

Расписание занятий для очных групп:

	№ урока	**Время**
Конкретный день недели согласовывается во время учебного процесса	1-2	09:30 - 11:00
	3-4	11:15 - 12:45
	5-6	13:45 - 15:15
	7-8	15:30 - 17:00

Рабочая программа

Модуль 1: Техники и инструменты криптографии.

- Жизненный цикл информационной безопасности.
- *Упражнение 1.1. Определение концепций и компонентов информационной безопасности.*
- Механизмы контроля.
- *Упражнение 1.2. Обсуждение механизмов контроля.*
- Методы аутентификации.
- *Упражнение 1.3. Обсуждение методов аутентификации.*
- Основы криптографии.
- *Упражнение 1.4. Обсуждение основ криптографии.*
- Политика безопасности.
- *Упражнение 1.5. Изучение политики безопасности.*

Модуль 2: Угрозы и уязвимости.

- Социальная инженерия.
- *Упражнение 2.1. Атаки социальной инженерии.*
- Вредоносное ПО.
- *Упражнение 2.2. Идентификация вредоносного ПО.*
- Угрозы ПО.
- *Упражнение 2.3. Идентификация атак на ПО.*
- Сетевые угрозы.
- *Упражнение 2.4. Классификация сетевых угроз.*
- Угрозы и уязвимости беспроводных сетей.
- *Упражнение 2.5. Обсуждение угроз, уязвимостей и защиты беспроводных сетей.*
- Физические угрозы и уязвимости.
- *Упражнение 2.6. Идентификация физических угроз и уязвимостей.*

Модуль 3: Управление безопасностью данных, приложений и хостов.

- Управление безопасностью данных.
- *Упражнение 3.1. Управление безопасностью данных.*
- Управление безопасностью приложений.
- *Упражнение 3.2. Настройка веб-браузера.*
- *Упражнение 3.3. Управление безопасностью приложений.*
- Управление безопасностью хостов и устройств.
- *Упражнение 3.4. Внедрение аудита.*
- *Упражнение 3.5. Защита сервера.*
- Управление безопасностью мобильных устройств.
- *Упражнение 3.6. Управление безопасностью мобильных устройств.*

Модуль 4: Безопасность сети.

- Механизмы защиты в сетевых технологиях и устройствах.
- *Упражнение 4.1. Настройка межсетевого экрана.*
- *Упражнение 4.2. Настройка системы обнаружения вторжений.*
- Компоненты системы защиты периметра сети.
- *Упражнение 4.3. Обзор компонентов систем защиты периметра сети.*
- Внедрение сетевых протоколов и служб.
- *Упражнение 4.4. Установка веб-сервера IIS.*

- *Упражнение 4.5. Защита сетевого трафика с помощью IPSec.*
- Применение принципов безопасного администрирования сети.
- *Упражнение 4.6. Защита маршрутизатора Windows Server 2012 R2.*
- *Упражнение 4.7. Защита файлового сервера.*
- Защита беспроводного трафика.
- *Упражнение 4.8. Защита беспроводного трафика.*

Модуль 5: Контроль доступа, аутентификация и управление учетными записями.

- Контроль доступа и службы аутентификации.
- *Упражнение 5.1. Резервное копирование Active Directory.*
- *Упражнение 5.2. Защита сервера удаленного доступа.*
- *Упражнение 5.3. Настройка аутентификации удаленного доступа.*
- Контроль управления учетными записями.
- *Упражнение 5.4. Внедрение контроля управления учетными записями.*

Модуль 6: Управление сертификатами.

- Создание иерархии удостоверяющих центров (далее УЦ).
- *Упражнение 6.1. Установка УЦ.*
- *Упражнение 6.2. Защита УЦ на основе Windows Server 2012 R2.*
- Выдача сертификатов.
- *Упражнение 6.3. Выдача сертификатов.*
- Защита сетевого трафика с помощью сертификатов.
- *Упражнение 6.4. Защита сетевого трафика с помощью сертификатов.*
- Обновление сертификатов.
- *Упражнение 6.5. Обновление сертификата УЦ.*
- *Упражнение 6.6. Обновление сертификата веб-сервера.*
- Резервное копирование, восстановление сертификатов и закрытых ключей.
- *Упражнение 6.7. Резервное копирование сертификата и закрытого ключа.*
- *Упражнение 6.8. Восстановление сертификата и закрытого ключа.*
- Отзыв сертификатов.
- *Упражнение 6.9. Отзыв сертификатов.*
- *Упражнение 6.10 изменение интервала публикации списка отозванных сертификатов.*

Модуль 7: Соответствие требованиям и безопасность операций.

- Физическая безопасность
- *Упражнение 7.1. Обзор компонентов физической безопасности*
- Соответствие требованиям законодательства
- У*пражнение 7.2. Соответствие требованиям законодательства*
- Повышение осведомленности персонала по вопросам ИБ
- *Упражнение 7.3. Повышение осведомленности персонала по вопросам ИБ*
- Интеграция систем и данных с контрагентами
- *Упражнение 7.4. Интеграция систем и данных с контрагентами*
- *Упражнение 7.5. Внедрение политики физической безопасности в организации.*

Модуль 8: Управление рисками.

- Анализ рисков.
- *Упражнение 8.1. Анализ рисков.*
- Методы и средства оценки уязвимостей.
- *Упражнение 8.2. Сбор сетевого трафика с помощью Microsoft Message Analyzer.*

- Выявление уязвимостей.
- *Упражнение 8.3. Сканирование портов.*
- *Упражнение 8.4. Сканирование уязвимостей паролей.*
- *Упражнение 8.5. Сканирование на наличие общих уязвимостей.*
- Техники отпугивания и минимизации рисков.
- *Упражнение 8.6. Мониторинг вторжений.*
- *Упражнение 8.7. Исследование ресурсов Интернета по ИБ.*

Модуль 9: Управление инцидентами ИБ, поиск и устранение неисправностей.

- Реакция на инциденты безопасности.
- *Упражнение 9.1. Реакция на инциденты безопасности.*
- Восстановление после инцидента безопасности.
- *Упражнение 9.2. Восстановление после инцидента безопасности.*
- *Упражнение 9.3. Исследование инцидентов безопасности.*

Модуль 10: Обеспечение непрерывности бизнеса и планирование восстановления после катастроф.

- Непрерывность бизнеса.
- *Упражнение 10.1. Обсуждение планирования непрерывности бизнеса.*
- Урок 10.2. Планирование восстановления после катастроф.
- *Упражнение 10.2. Создание плана восстановления после катастроф.*
- Урок 10.3. Исполнение процедур и плана восстановления.
- *Упражнение 10.3. Исполнение процедур и плана восстановления.*
- *Упражнение 10.4. Исследование непрерывности бизнеса и восстановления после катастроф.*

Модуль 11: Знакомство с экзаменом.

Модуль 12: Итоговый тест.

Организационно-педагогические условия реализации Программы

При реализации Программы применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, использовании различных образовательных технологий, в том числе дистанционных образовательных технологий и электронного обучения.

Организационные условия реализации программы в разных формах обучения регулируются следующими локальными нормативными актами:

- Положение об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».
- Положение о порядке применения электронного обучения, дистанционных образовательных технологий в НОЧУ ДПО УЦ «Сетевая Академия».

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 в порядке, установленном Положением о библиотеке в НОЧУ ДПО УЦ «Сетевая Академия».

Занятия по Программе проводятся преподавателями, предварительно подтвердившими свою квалификацию. В числе базовых требований ко всем преподавателям – требование обязательного прохождения программы «Андрагогика. Эффективное обучение взрослых» в форме учебного курса и пробной лекции, а также сдачи технических сертификационных тестов по продукту или технологии, рассматриваемым в курсе.

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 НОЧУ ДПО УЦ «Сетевая Академия».

Освоение Программы завершается итоговой аттестацией обучающихся в форме, определенной учебным планом, и в порядке, установленном Положением об организации образовательного процесса в НОЧУ ДПО УЦ «Сетевая Академия».

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 промежуточных тестов после изучения каждого модуля.

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

Контрольные вопросы для оценки знаний и навыков слушателей задаются и выполняются в следующих областях:

- Основы ИБ.
- Угрозы и уязвимости
- Управление безопасностью данных, приложений и хостов.
- Безопасность сети.
- Контроль доступа, аутентификация и управление учетными записями.
- Управление сертификатами
- Соответствие требованиям и безопасность операций.
- Управление рисками.
- Управление инцидентами ИБ, поиск и устранение неисправностей.
- Обеспечение непрерывности бизнеса и планирование восстановления после катастроф.