# CCNA Security 2.0
# Общий объем и последовательность изучения

**Последнее обновление: декабрь 6, 2017**

## Целевая аудитория

Курс Cisco CCNA® Security разработан для учащихся Сетевой академии Cisco®, которые хотели бы начать работать в области информационной безопасности. Целевая аудитория – студенты, обучающиеся по технологическим программам в институтах и университетах, и ИТ-специалисты, которые хотели бы расширить свои базовые навыки в области маршрутизации и коммутации.

Курс CCNA – это следующий шаг для учащихся, которые уже прошли курсы CCENT или CCNA Routing and Switching и которые бы хотели усовершенствовать свои навыки, чтобы начать успешно работать в области сетевой безопасности.

## Обязательные требования

Слушатели курса CCNA Security должны уже обладать следующими навыками и знаниями:

- Знания и навыки в области сетевых технологий на уровне CCENT
- Базовые навыки работы с ПК и Интернетом

## Цели сертификации

Программа курса CCNA Security готовит слушателей к сертификационному экзамену Implementing Cisco Network Security (IINS) (210-260), после которого можно получить сертификацию CCNA Security.

## Описание программы

Курс CCNA Security дает учащимся знания и навыки, необходимые им для подготовки к началу карьеры специалистов по безопасности начального уровня. Данный курс является практическим и профессионально ориентированным решением для электронного обучения. В ходе обучения повышенное внимание уделяется получению практического опыта. Программа курса комбинированная: онлайн-обучение сочетается с занятиями в аудитории. Цель курса CCNA Security – дать глубокое понимание принципов сетевой безопасности, а также инструментов и конфигураций, необходимых для обеспечения безопасности сети.

В ходе разных лабораторных работ учащиеся получат практический опыт работы, включая опыт устранения неисправностей, правильного использования навыков и построения моделей. Все лабораторные работы настоящего курса могут выполняться на реальном физическом оборудовании или с помощью решения NETLAB группы NDG. Большинство глав включает задачи использования навыков в программе Packet Tracer, при этом упражнения становятся все сложнее по ходу курса, так как в них учащиеся будут использовать все приобретенные ранее навыки.

## Цели программы

Курс CCNA Security позволяет учащимся получить навыки, необходимые им для начала работы в качестве специалистов сетевой безопасности начального уровня и для получения сертификата CCNA Security. Курс содержит теоретическую и практическую информацию по основам сетевой безопасности. Материал излагается в логической последовательности, на основе технологий.

Цели курса CCNA Security:

- Обеспечение глубокого теоретического понимания сетевой безопасности
- Обучение учащихся навыкам и знаниям, необходимым для проектирования и поддержки систем сетевой безопасности
- Знакомство с практическим опытом с учетом отраслевых особенностей для подготовки учащихся к работе в сфере сетевой безопасности и выполнению работ на начальном уровне в конкретных отраслях
- Предоставление учащимся возможности практической работы на ИТ-оборудовании для подготовки их к сдаче сертификационных экзаменов и последующей работе в качестве специалистов по сетевой безопасности

Закончив курс CCNA Security, учащиеся смогут выполнять следующие задачи:

- Объяснять, что такое сетевые угрозы, техники нейтрализации и основы безопасности сети
- Защищать административный доступ к маршрутизаторам Cisco
- Защищать административный доступ с использованием AAA
- Внедрять технологи межсетевых экранов для защиты периметра сети
- Конфигурировать IPS для нейтрализации атак на сеть
- Описывать факторы, которые необходимо учитывать для обеспечения безопасности LAN, и внедрять функции безопасности уровня 2 и оконечных устройств
- Описывать способы обеспечения конфиденциальности и целостности данных
- Внедрять безопасные виртуальные частные сети (VPN)
- Внедрять конфигурацию межсетевого экрана ASA с использованием интерфейса командной строки (CLI)
- Внедрять конфигурацию межсетевого экрана ASA и сетей VPN с использованием ASDM
- Проверять безопасность сети и создавать техническую политику безопасности

## Минимальные системные требования

Требования программы курса CCNA Security:

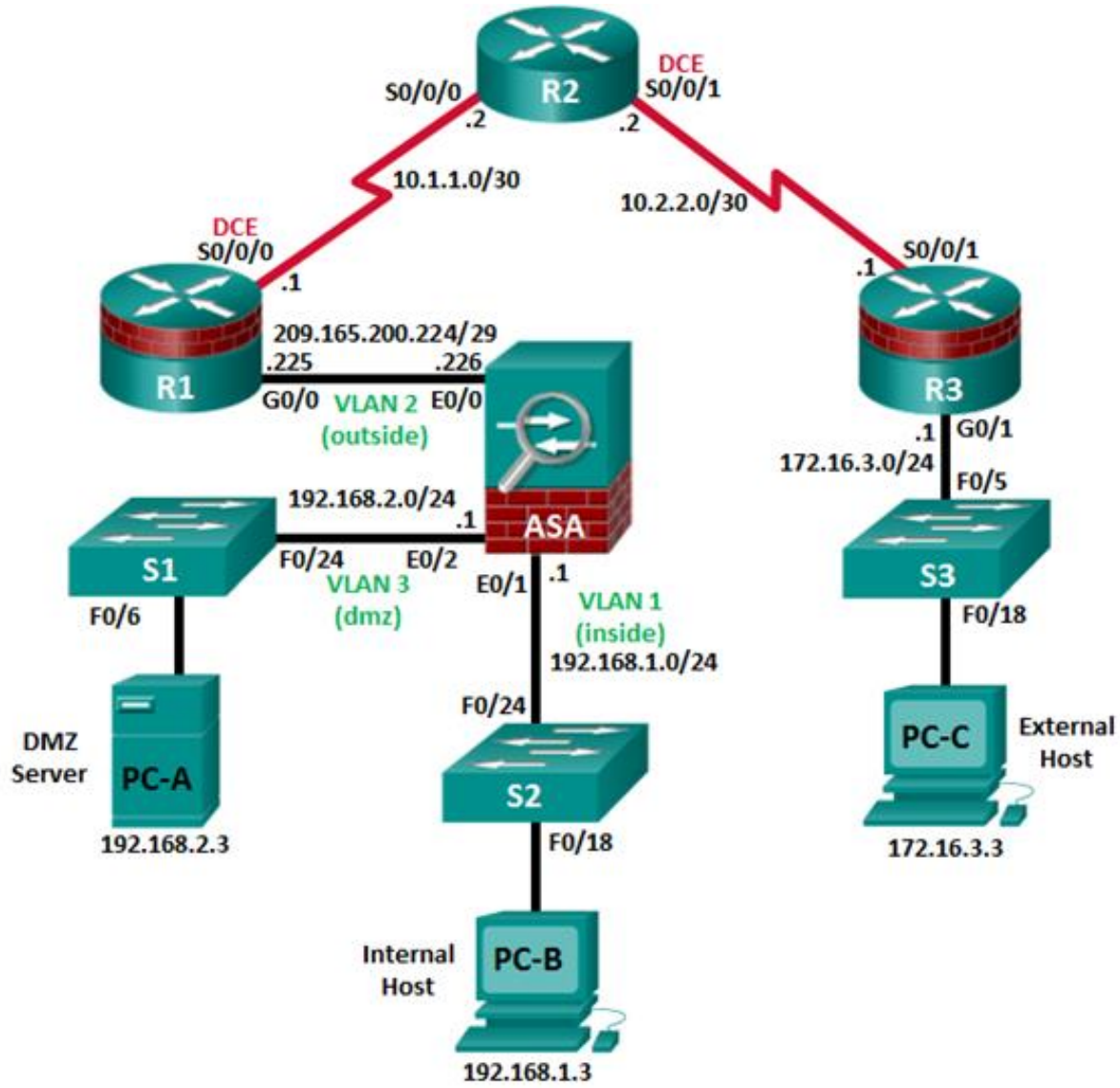
- 1 ПК на учащегося

Требования к комплекту для лабораторных работ по курсу CCNA Security

Подробную информацию об оборудовании, включая описания и номера компонентов, см. на странице Equipment Information на портале Cisco Netspace. В этом документе вы сможете посмотреть новейшую информацию, включая технические характеристики, для следующего оборудования, требуемого для курса:

- 3 маршрутизатора Cisco, 2 с лицензией Security Technology Package
- 3 двухпортовые платы последовательного интерфейса WAN
- 3 коммутатора Cisco
- Одно многофункциональное устройство безопасности Cisco ASA
- Разные кабели Ethernet, последовательные кабели и концентраторы

На оборудовании должна быть настроена следующая конфигурация:



## Обзор курса CCNA Security

На этом курсе учащиеся получат навыки, необходимые им для получения возможности работы в сфере информационной безопасности на начальном уровне. Курс дает возможность на практике познакомиться с работой специалиста по сетевой безопасности. Инструкторам рекомендуется приводить примеры из реальной жизни и делиться опытом своей работы вне класса.

## Содержание главы

**Таблица 1.** Содержание главы

| Глава/раздел | Цели/задачи |
|---|---|
| **Глава 1. Современные угрозы сетевой безопасности** | **Объяснение того, что такое сетевые угрозы, техники нейтрализации и основы безопасности сети** |
| 1.1 Защита сетей | Объяснение безопасности сети |
| 1.2 Сетевые угрозы | Описание угроз и атак разного типа |
| 1.3 Нейтрализация угроз | Объяснение инструментов и процедур для нейтрализации последствий воздействия вредоносного ПО и распространенных сетевых атак |
| **Глава 2. Обеспечение безопасности сетевых устройств** | **Защита административного доступа к маршрутизаторам Cisco** |
| 2.1 Защита доступа к устройствам | Конфигурирование безопасного административного доступа |
| 2.2 Назначение административных ролей | Конфигурирование авторизации команд с использованием уровней привилегий и CLI на основе ролей |
| 2.3 Мониторинг устройств и управление ими | Внедрение защищенного управления и мониторинга сетевых устройств |
| 2.4 Использование автоматических функций обеспечения безопасности | Использование автоматических функций для обеспечения безопасности на маршрутизаторах под управлением IOS |
| **Глава 3. Аутентификация, авторизация и учет** | **Защита административного доступа с использованием AAA** |
| 3.1 Назначение AAA | Объяснение способов применения AAA для защиты сети |
| 3.2 Локальная аутентификация AAA | Внедрение аутентификации AAA, в ходе которой выполняется сверка пользователей с локальной базой данных |
| 3.3 Серверное решение AAA | Объяснение серверной аутентификации AAA и ее коммуникационных протоколов |
| 3.4 Серверная аутентификация AAA | Внедрение серверной аутентификации с использованием протоколов TACACS+ и RADIUS |
| 3.5 Серверная авторизация и учет AAA | Конфигурирование серверной авторизации и учета AAA. |
| **Глава 4. Внедрение технологий межсетевого экрана** | **Внедрение технологий межсетевого экрана для защиты периметра сети** |
| 4.1 Списки контроля доступа | Внедрение списков контроля доступа (ACL) для фильтрации трафика и нейтрализации сетевых атак |
| 4.2 Технологии межсетевых экранов | Настройка классического межсетевого экрана для нейтрализации сетевых атак |
| 4.3 Зональные межсетевые экраны | Внедрение зонального межсетевого экрана с использованием интерфейса командной строки (CLI) |
| **Глава 5. Внедрение системы предотвращения вторжений** | **Конфигурирование IPS для нейтрализации атак на сеть** |
| 5.1 Технологии IPS | Объяснение способов применения AAA для защиты сети |
| 5.2 Сигнатуры IPS | Объяснение способов применения сигнатур для обнаружения вредоносного сетевого трафика |
| 5.3 Внедрение IPS | Конфигурирование операций Cisco IOS IPS с использованием интерфейса командной строки (CLI). |
| **Глава 6. Обеспечение безопасности локальной сети (LAN)** | **Описание факторов, которые необходимо учитывать для обеспечения безопасности LAN, и способов внедрения функций безопасности уровня 2 и оконечных устройств** |
| 6.1 Безопасность оконечных устройств | Объяснение уязвимостей оконечных устройств и способов защиты |
| 6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на уровне 2 | Внедрение функций безопасности на уровне 2 |
| **Глава 7. Криптографические системы** | **Описание методов обеспечения конфиденциальности и целостности данных** |
| 7.1 Криптографические сервисы | Объяснение способов совместного применения типов шифрования, хешей и цифровых подписей для обеспечения конфиденциальности, целостности и аутентификации |
| 7.2 Обеспечение базового уровня целостности и аутентификации | Объяснение способов применения криптографических хешей для обеспечения целостности и аутентификации данных |
| 7.3 Конфиденциальность | Объяснение способов применения алгоритмов шифрования для обеспечения конфиденциальности данных |
| 7.4 Криптография с открытыми ключами | Объяснение способов применения инфраструктуры открытых ключей для обеспечения конфиденциальности и аутентификации данных |

| Глава/раздел | Цели/задачи |
|---|---|
| **Глава 8. Внедрение виртуальных частных сетей (VPN)** | **Внедрение защищенных виртуальных частных сетей (VPN)** |
| 8.1 Сети VPN | Объяснение назначения сетей VPN |
| 8.2 Компоненты сети IPsec VPN и их функционирование | Объяснение принципа работы сетей IPsec VPN |
| 8.3 Реализация сетей Site-to-Site IPsec VPN с помощью CLI | Конфигурирование сети Site-to-Site IPsec VPN (между двумя пунктами) с аутентификацией с помощью общего ключа с использованием интерфейса командной строки (CLI) |
| **Глава 9. Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance** | **Внедрение конфигурации межсетевого экрана ASA с использованием интерфейса командной строки (CLI)** |
| 9.1 Знакомство с ASA | Объяснение того, как устройство ASA функционирует в качестве расширенного межсетевого экрана с сохранением состояния. |
| 9.2 Конфигурация межсетевого экрана ASA | Внедрение конфигурации межсетевого экрана ASA |
| **Глава 10. Многофункциональное устройство обеспечения безопасности Cisco ASA с расширенным функционалом** | **Внедрение конфигурации межсетевого экрана ASA и сетей VPN с использованием ASDM** |
| 10.1 ASA Security Device Manager | Внедрение конфигурации межсетевого экрана ASA |
| 10.2 Настройка VPN в ASA | Настройка сетей VPN удаленного доступа на устройстве ASA |
| **Глава 11. Управление безопасной сетью** | **Проверка безопасности сети и создание технической политики безопасности** |
| 11.1 Тестирование безопасности сети | Объяснение разных методов и инструментов, используемых для тестирования безопасности сети |
| 11.2 Разработка комплексной политики безопасности | Объяснение назначения комплексной политики по информационной безопасности |


Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410,
факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230,
факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600,
факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691,
факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101,
факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820,
факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460,
факс: +998 (71) 140 4465