Cisco

EC-Council

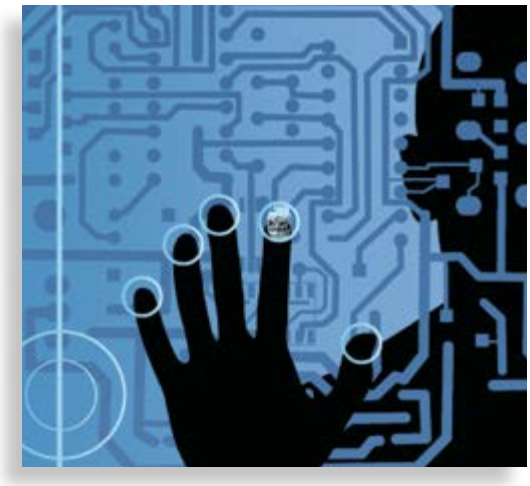
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Рекомендуемые курсы обучения

2013

ЭВРИКА

Выбери путь – будь в безопасности



Мир меняется. Растет скорость обработки информации, и в соответствии с расширенным законом Мура сложность ИТ-систем удваивается каждый год. Современные информационные системы переводят количество данных в качество производимых продуктов и предоставляемых услуг, превращая гигабайты разрозненной информации в аналитические отчеты, тенденции и прогнозы. Всё больше растет зависимость бизнеса от средств ИТ-технологий, и если какая-то из систем выйдет из строя, организация понесёт большие финансовые потери. И при этом количество угроз неизменно растёт.

По данным «Лаборатории Касперского» каждый день на свет появляется более 40 тысяч новых вирусов, практически каждый день производители выпускают десятки критических патчей для популярных программ, и каждый день специалисты по информационной безопасности находят новые уязвимости в современных операционных системах.

Информационные системы нового поколения должны быть «мягкими» – должны легко интегрироваться с новыми программными и аппаратными продуктами, быть динамичными и адаптироваться под нужды бизнеса. Но имеющиеся системы безопасности, защищающие информационные системы от вредоносного воздействия, на данный момент, продолжают быть «жёсткими» – настроенными на строго определенную модель угроз, где новые неучтенные элементы либо игнорируются и остаются незащищенными, либо запрещаются.

Старые средства безопасности не справляются, они не предусматривали введение новых мобильных устройств в закрытую корпоративную систему. Но обычно сотрудники стремятся использовать свои телефоны, подключать к информационной системе компании свои мобильные устройства и обрабатывать корпоративные данные на своих личных компьютерах. А контролировать личные устройства сотрудников системе безопасности невероятно сложно. При этом риск кражи или потери конфиденциальной информации при обработке на незащищенных устройствах увеличивается в десятки раз. Поэтому необходимо менять подход к построению систем безопасности.

Время простых решений прошло. Теперь недостаточно раз и навсегда запретить выход в глобальную сеть, поставить межсетевой экран, установить антивирусную программу и чувствовать себя защищенными. Безопасность – это процесс, а не результат, и процесс обеспечения безопасности должен быть непрерывным, динамичным и эффективным. Нужно обеспечить постоянную во времени защиту систем и сетей, способную расширяться, охватывая новые модули, и изменяться в зависимости от потребностей бизнеса, обеспечивать безопасность конфиденциальной информации.

Современная система – это совокупность устройств, программ и людей, тесно взаимодействующих между собой. Поэтому для обеспечения безопасности необходимы комплексные решения, которые будут учитывать неоднородность компонентов, составляющих информационную систему. Полноценное комплексное решение по организации защиты информационной системы компании должно контролировать влияние на систему оборудования, программного обеспечения и персонала, потому как ошибки и нестабильности в работе каждого из составляющих могут создать угрозу безопасности системы в целом.

Информационные системы связаны с человеком; без людей техника не работает. Но люди являются самым слабым звеном в цепочке безопасности, осознано или бессознательно разрушающие стройную систему безопасности. Поэтому одна из задач системы безопасности снизить это влияние, но без качественной подготовки и соответствующего образования сотрудник может погубить информационную систему компании, поставить под угрозу конфиденциальные данные и работоспособность ресурсов.

Поддерживать безопасность организации должны все, начиная от уборщицы, которая может оставить ключи от режимных помещений в публичной зоне, и до генерального директора, определяющего политику безопасности. Угрозу информационной системе компании может создать любой сотрудник, поэтому необходимо обеспечить понимание и соблюдение персоналом элементарных требований безопасности.

Компетентность людей в вопросах поддержания безопасности определяется образованием и практическим опытом работы с подобными системами. Но если непосредственный опыт отсутствует, не хватает необходимых знаний и навыков, то решить этот вопрос можно с использованием виртуальной симулирующей среды, пока критическая ситуация не появилась в реальности и не повлекла за собой серьёзные финансовые потери.

Учебный центр компании «Эврика» с 1999 года специализируется на подготовке высококвалифицированных ИТ-специалистов и имеет статус авторизованного учебного центра от компаний Microsoft, Novell, Red Hat, Cisco, EC-Council. По нашему опыту можно отметить, что ранее вопросы безопасности покрывались отдельными модулями в составе авторизованных курсов по популярным направлениям. Но теперь картина изменилась. Сложность систем дошла до уровня, когда проявилась необходимость отдельных курсов по решению вопросов обеспечения безопасности.

Предоставить полную и исчерпывающую информацию по всем вопросам безопасности в компактном виде весьма проблематично. Поэтому здесь разобраны основные направления, определяющие наибольшее число уязвимостей в системе безопасности. Направление работы с людьми, как пользователями, так и администраторами, достаточно полно раскрыто в отдельных курсах известной интернациональной организации EC-Council, а построение архитектуры сети, настройка и администрирование сетевого оборудования глубоко и подробно освещены в специализированных учебных программах компании Cisco.

Учитывая потребности рынка, мировой лидер в области безопасности организация EC-Council разработала специальные курсы для пользователей и системных администраторов, позволяющие рассмотреть известные уязвимости в компьютерных системах и познакомиться с программами и методами, которые применяют злоумышленники для взлома компьютерных систем. Одним из ярких показателей качества учебных программ EC-Council является аккредитация курсов Американским институтом национальных стандартов (ANSI), что позволяет использовать данные учебные программы для подготовки сотрудников правительственных военных учреждений США, в том числе и Пентагона.

Компания Cisco, признанный лидер в производстве качественного сетевого оборудования, разработала ряд обучающих курсов, позволяющих глубоко понимать архитектуру сети и использовать эти знания для установки и настройки средств сетевой безопасности, таких как аппаратные межсетевые экраны, системы противодействия вторжениям, фильтрация трафика и многих других полезных функций, непосредственно применяемых к сетевому оборудованию Cisco.

EC-Council и Cisco используют современный подход для обучения новым технологиям, привлекая возможности виртуальных сред и последних наработок в своей области. Подобные курсы позволяют в сравнительно короткие сроки получить знания и навыки для построения эффективных, динамичных и отказоустойчивых систем, отвечающих всем требованиям безопасности.

Таким образом, обучая персонал корректной и безопасной работе с информационной системой, можно защитить организацию от современных методов атак и снизить риски потенциальных угроз. Использование проверенного, стандартизированного и актуального материала позволяет гарантировать высокое качество обучения и наибольшую результативность по окончанию курсов.

Обучение не является обязательным условием успешного развития компании, но оно может серьёзно облегчить повседневное взаимодействие с информационной системой и перераспределить бюджетные расходы в сторону развития и расширения бизнеса, сократив непредсказуемые риски со стороны информационной безопасности. Обучение – самый дешевый и эффективный способ добиться результата, но данный способ нужно использовать вовремя.

Факты

Согласно отчету об анализе информационной безопасности, проводившемся в течении 2012 года компанией Check Point:

✓ в 63% компаний хотя бы 1 система заражена вредоносным ПО;

✓ в 29% компаний была обнаружена передача через сеть Интернет данных кредитных карт;

✓ в 80% компаний было обнаружено использование публичных файловых хранилищ (таких как Dropbox).

Согласно отчету по информационной безопасности Cisco:

✓ вредоносный контент можно «подцепить» на сайтах интернет-магазинов в 21 раз чаще (а в поисковых механизмах – в 27 раз чаще), чем на сайтах, специально созданных хакерами;

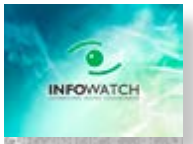
✓ только 40% сотрудников знают об официальных правилах использования на работе личных устройств;

✓ более 70% сотрудников, даже зная о наличии корпоративных правил, не придерживаются их в своей повседневной работе;

✓ 66% сотрудников считают, что IT-специалисты не имеют права следить за их поведением в сети, даже если это поведение связано с использованием корпоративных устройств в корпоративных сетях;

✓ 75% сотрудников готовы пойти на риск, выкладывая личную информацию, например, номера кредитных карт и личные контактные данные, если это может приносить какую-то выгоду или удобство.

По результатам исследования, проведенным аналитическим центром компании InfoWatch:



✓ за 2012 год в России зафиксировано и обнародовано в 5 раз больше утечек, чем годом ранее;

✓ 77% утечек относятся к разряду злонамеренных;

✓ 65% утечек – персональные данные;

✓ 38% утечек приходятся на госучреждения. При этом доля утечек из коммерческих организаций – 47%.

Тенденции

Согласно многим фактам, можно оценить характерные направления для изменений в системах информационного обмена. Эти изменения затрагивают и технические, и социальные, и экономические стороны взаимодействий.

В процессе формирования угроз безопасности наметились следующие тенденции:

✓ труднее становится идентифицировать потенциальные источники опасности – сегодня, как отмечают специалисты Cisco, сетевые злоумышленники фокусируют внимание не столько на порнографических, фармацевтических и игровых сайтах, сколько на обычных сетевых ресурсах с массовой аудиторией, как, например, популярные поисковые механизмы, розничные магазины и социальные сети;

✓ выявляется неприятие мер контроля со стороны нового поколения сотрудников – современное поколение испытывает на прочность корпоративную культуру и политику компании в области безопасности, требуя от работодателя свободы использования социальных сетей, личных устройств и методов мобильной работы (при этом гораздо спокойнее относясь к отслеживанию их работы в сети со стороны аналитических сервисов, чем со стороны IT-специалистов компании-работодателя);

- ✓ проявляется небрежное отношение к приватности информации – в российских компаниях преобладающим фактором риска является халатность в отношении политик информационной безопасности со стороны рядовых сотрудников;
- ✓ вырастает число мобильных устройств, распространяется концепция BYOD – информационная безопасность компаний становится уязвимой из-за того, что сотрудники стремятся к повсеместному применению мобильных устройств, которые используются и в личных, и в корпоративных целях;
- ✓ сотрудники стремятся к мобильности и использованию беспроводной связи – мобильность увеличивает производительность труда (согласно Cisco IBSG Horizons Research) и, как следствие, предоставляет компаниям конкурентные преимущества, помогая привлечь новых заказчиков и повысить качество оказываемых услуг;
- ✓ консолидируется хакерское сообщество – хакеры объединяются в группы, у них теперь иные задачи, иные цели, иные подходы. И, значит, должны меняться способы нейтрализации их угроз;
- ✓ активизируется государственный контроль – на данный момент ярко выражено стремление правоохранительных органов и иных государственных силовых структур опережать киберпреступников, используя различные средства слежения;
- ✓ вырастает число вирусов для мобильных устройств – эксперты отмечают лавинообразный рост числа вредоносных программ для мобильной платформы Android.

Целесообразность

Современным компаниям нужно внимательно относиться к проблемам информационной безопасности, так как утечки конфиденциальной информации могут привести к ощутимым убыткам в виде штрафов, недополученной прибыли, потери привилегированного положения на рынке и т.п. Новое видение бизнеса, новые методы и технологии определяют жизнеспособность современной организации. Конкуренты идут на многое, используя все имеющиеся средства и возможности, чтобы получить интересующие их сведения о прогрессивной компании, включая:

- ✓ информацию о потенциальных клиентах и сделках;
- ✓ клиентские базы и непосредственно клиентов;
- ✓ стратегические планы компаний относительно освоения новых рынков;
- ✓ планы разработки и вывода на рынок новых продуктов;
- ✓ конфиденциальную информацию о ключевых сотрудниках;
- ✓ уровень зарплат сотрудников и существующих в компании премий, а также политики поощрения;
- ✓ разработки, имеющиеся в компаниях (коды программ, чертежи, алгоритмы).

Вне зависимости от типа организации, современные эффективные предприятия функционируют на базе различного рода информационных и вычислительных систем. Бесперебойная работа этих систем нуждается в защите их от вредоносных и непредумышленных вмешательств, которое может нанести даже материальный ущерб: например, в августе прошлого года в ходе атаки Shamoon было выведено из строя более 30 тыс. компьютеров крупной нефтяной компании Saudi Aramco.

Предприятия государственного сектора и военно-промышленного комплекса, а также бюджетные организации обязаны соблюдать законодательные требования к защите информации. Достижения информационных технологий применяются не только для шпионажа, но и в диверсионных целях, поэтому необходимо обеспечить корректную работу системы защиты информации для противодействия атакам и снижения рисков.

Неизбежность

Дополнительной угрозой информационной безопасности становятся личные устройства пользователя в сети организации. Набирает силу концепция BYOD – Bring Your Own Device. Строго говоря, BYOD – это, как правило, не полноценное законченное решение, а набор политик, обеспечивающих безопасность компании и распределение пользователей по категориям доступа к определенным ресурсам по различным параметрам.

Согласно исследованиям Cisco, в России концепцию BYOD так или иначе используют 55% работников умственного труда. Кроме того, когда сотрудники получают право по своему усмотрению выбирать место для работы, методы ведения бизнеса и инструментарий, уровень их удовлетворенности работой повышается, а работодатель сокращает издержки.

Пока личные мобильные устройства сотрудников не наносят заметного урона корпоративной безопасности, на них просто не обращают внимания. Но как только урон превышает некий приемлемый для компании уровень, их тут же запрещают.

Феномен BYOD с возрастающим использованием планшетов и смартфонов в корпоративной инфраструктуре серьезно изменил рабочую среду организаций. Существуют различные решения по внедрению концепции BYOD, например, у Citrix или Cisco. Так, архитектура Cisco «Сети без границ» с комплексным подходом к управлению устройствами, политике безопасности и мобильности представляет собой наиболее полное решение в отрасли, которое отвечает требованиям данного тренда.

Консолидация ресурсов информационной безопасности служит базой для перехода к централизованному управлению системой безопасности. При этом приоритеты в обеспечении корпоративной информационной безопасности смещаются в сторону защиты критических данных и повышения надежности информационных систем.

Подход

Безопасность сегодня не может зависеть только от одной, пусть даже и самой лучшей системы защиты. Необходим целый комплекс защитных механизмов и организационных мер, направленных на выявление, нейтрализацию угроз и предотвращение их повторов в будущем. Это проактивный режим защиты, без которого информационная безопасность в современных условиях неэффективна, если не сказать невозможна.

Как никогда важен архитектурный подход в области защиты корпоративных или ведомственных сетей, позволяющий перекрывать различные каналы проникновения вредоносных программ внутрь защищаемого виртуального пространства. Поэтому специалисты давно пропагандируют не точечную защиту, а систему эшелонированной обороны, состоящей из множества взаимоувязанных элементов.

В современном мире ни одна система защиты не будет эффективной длительное время без постоянной подпитки знаниями о новых способах совершения атак. И такое обновление средств защиты должно происходить непрерывно, а не раз в неделю, не раз в день, и даже не раз в час.

Нужно также определять статус безопасности устройства. Каждый раз, когда новое устройство пытается подключиться к корпоративной сети, необходимо проверить, какая на устройстве операционная система, есть ли там антивирус, обновлена ли система и база

данных и т. д. Если же какой-то из компонентов не обнаруживается, его можно предложить загрузить.

Кроме того, нужно определять место, откуда пользователь заходит в сеть: из офиса компании или удаленно, например, через VPN. Так выйдя, допустим, в любое кафе, где есть публичная сеть Wi-Fi, сотрудник может по-прежнему получать доступ к информации через VPN, создав угрозу проникновения в закрытую сеть организации через незащищенное подключение. Весьма полезно ввести некие политики, которые при удаленном доступе позволяют войти в корпоративную сеть, но блокируют самые «чувствительные» зоны (например, записи о финансах компании).

Так или иначе, все упомянутые возможности при вдумчивом проектировании решения предоставляют возможность формировать мощную иерархию политик раздельного доступа к корпоративным ресурсам и контроля за обменом трафиком с внешним миром с учетом массы факторов, влияющих на безопасность компании.

Одним из решений задачи построения комплексной системы безопасности будет платформа Cisco Identity Services Engine (ISE), позволяющая внедрить концепцию использования собственных устройств (BYOD) среди сотрудников или организовать более безопасный доступ к ресурсам центра обработки данных.

Технические и программные средства Cisco, обеспечивающие системную защиту ресурсов компании, в том числе при реализации BYOD, включают в себя:

- ✓ платформу Cisco Identity Services Engine ISE;
- ✓ адаптивные устройства безопасности Cisco ASA;
- ✓ устройства предотвращения вторжений Cisco IPS;
- ✓ устройства контроля доступа к сети Cisco NAC;
- ✓ серверы контроля доступа Cisco ACS;
- ✓ устройства защиты www-траффика Cisco WSA, ESA;
- ✓ клиентские решения Cisco AnyConnect, Virtual Office;
- ✓ устройства мобильных сервисов Cisco MSE.

Cisco ISE — это платформа, работающая с учетом контекста местоположения и на основе идентификации. Она собирает информацию о сети, пользователях и устройствах в режиме реального времени и затем использует эту информацию для принятия упреждающих решений по управлению, обеспечивая применение политик в пределах всей сетевой инфраструктуры.

Платформа Cisco Identity Service Engine является основным компонентом решения Cisco **TrustSec** и архитектуры **Cisco SecureX**.

Решение

Каждая компания должна понимать текущую ситуацию – защитить себя нужно самостоятельно. С наименьшими затратами и наибольшей эффективностью. А для этого нужно понимать механизмы возникновения угроз и методы противодействия атакам.

Безусловно, необходимо позаботиться о действиях рядовых пользователей, по незнанию или халатности представляющие собой наиболее уязвимое звено в цепочке безопасности организации.

Для качественного обеспечения безопасности компании нужно учесть наиболее полный объем возможных угроз и разработать меры противодействия злоумышленникам.

В сложившейся ситуации опасность подстерегает компанию с разных сторон. ИТ-инфраструктура сложна и разнообразна, что серьезно затрудняет построение системы защиты и требует поддержки высококлассных специалистов. И даже это не гарантирует абсолютной безопасности вашей системы.

Давайте рассмотрим основные направления, откуда можно ожидать угрозы, что необходимо учесть при построении мощной системы безопасности.

Во-первых, необходимо исключить вопросы, связанные с оборудованием – это настройки по умолчанию для коммутаторов и маршрутизаторов, активные неиспользуемые службы на шлюзах и аппаратных брандмауэрах, открытые стандартные порты и работа сервисов на хорошо известных портах.

Здесь нужно менять дефолтные параметры оборудования, сменить пароли на управление устройствами, отключить дополнительные особенности аппаратного обеспечения, которые непосредственно не используются в вашей сети. Также необходимо закрыть все порты, которые не принимают участие в поддержке сетевого взаимодействия, и отключить все лишние сетевые сервисы.

Во-вторых, исключаем угрозы со стороны программного обеспечения – это любой вредоносный код, способный записаться и выполниться на вашем компьютере: вирусы, черви, трояны, программы-шпионы и спамеры, угрожающие конфиденциальности вашей информации и состоянию ее целостности, а также снижающие производительность ваших рабочих станций и пропускную способность сети.

Для противодействия таким угрозам нужно в обязательном порядке использовать антивирусное программное обеспечение, а также на системном уровне запретить выполнение неподписанных доверенным сертификатом или загруженных с неизвестного узла файлов или программ, централизованно настроить параметры операционных систем без возможности изменения их со стороны пользователя. Кроме этого, важно настроить систему мониторинга за производительностью рабочих станций, позволяющую вовремя идентифицировать вторжение в систему и качественно противодействовать злоумышленнику.

В-третьих, учитываем человеческий фактор – рядовые пользователи представляют собой самое слабое звено в системе безопасности. Некомпетентные сотрудники могут разглашать конфиденциальные данные компании или имя своей учетной записи и пароль; не понимая важность правил безопасности, многие пользователи пренебрегают рекомендациями ИТ-службы и подвергают опасности ресурсы и системы организации; или наоборот, получив вознаграждения от конкурентов, сотрудники компании становятся инсайдерами, предоставляющими важную внутреннюю информацию посторонним.

Взаимодействие с человеком – наиболее сложная часть построения системы безопасности, поэтому необходимо доходчиво объяснить пользователям, почему крайне важно следовать рекомендациям службы безопасности, рассказать, какие угрозы и провокации могут подстерегать их при взаимодействии с интернет-ресурсами и посторонними людьми, интересующимися вашей организацией. А для противодействия инсайдерам необходимо установить внутреннюю политику безопасности, распространяющуюся не только на рабочие станции, но и на сотрудников; нужно определить внутренние стандарты по работе с информацией и на уровне приказов регламентировать действие персонала.

Итак, теперь понятно, с какими задачами сталкивается специалист по информационной безопасности. И для успешного решения этих задач необходимо иметь знания о ситуации, либо с теории, либо из практики. Тогда возникает вопрос – где знания взять?

Как удовлетворить жажду знаний в тонких материях информационной безопасности? Безусловно, можно самостоятельно по крупицам собирать данные в глобальной сети, набивать шишки практического опыта и ловить каждое слово местного гуру, но, когда нужно получить за короткий срок систематизированную картину угроз и мер противодействия в современном мире, разумнее обратиться к сертифицированным профессионалам, готовым поделиться своими знаниями и навыками.

Средства

Лучший способ быстро и качественно получить необходимые для повседневной работы знания – это посетить специализированные обучающие курсы. Давайте посмотрим, какие курсы по обеспечению безопасности можно найти на рынке обучения.

На текущий момент выбор невелик – курсы международной организации EC-Council, специализирующейся в аттестации навыков обеспечения информационной безопасности, курсы базовой подготовки известной организации CompTIA и различные авторские курсы. Рассмотрим каждый из вариантов подробнее.

Авторские курсы довольно серьёзно зависят от компетенции своего автора-составителя. Безусловно, можно встретить профессионала высшей категории, жаждущего поделиться своим невероятным опытом, но чаще всего авторские курсы похожи на свалку несистематизированной информации. Кроме этого, необходимо самостоятельно следить за состоянием статусов инструктора и наводить справки о его компетенции.

Авторизованные курсы предоставляют возможность снять груз ответственности с плеч клиента и переложить обязанности отслеживания статуса и авторизации тренера на вендора курсов. Таким образом, можно быть уверенным, что авторизованные курсы читают квалифицированные профессионалы, качественно подготовлена лабораторная среда и материал курса проверен и одобрен коллективом авторов и рецензентом в компании, чья основная деятельность связана с обучением по нужному направлению.

Итак, кто же предлагает авторизованные курсы по безопасности? На российском рынке широкую известность получили две интернациональные компании – EC-Council и CompTIA, каждая из которых занимает свою нишу.

Ассоциация CompTIA (Computing Technology Industry Association) была создана в 1982 и является ведущим в мире поставщиком нейтральных к производителям сертификаций. Это значит, что сертификации CompTIA проверяют знания кандидата в целом по предмету, а не конкретные технологии отдельного поставщика. В дополнение к профессиональной сертификации, CompTIA поддерживает и остается мировым лидером ИТ-индустрии в области образования, пропаганды и благотворительных инициатив.

CompTIA предлагает базовые направления, позволяющие официально подтвердить фундаментальные знания, основы информационных технологий. В сфере безопасности и сетей довольно популярны направления Security+ и Network+, аттестующие кандидата как начинающего специалиста в области ИТ-безопасности и построения сетей. При этом подразумевается, что в дальнейшем кандидат продолжит получать сертификации более высокого уровня у других вендоров.

Авторизованные курсы CompTIA готовят слушателей к сдаче экзамена в тестовой форме, предоставляя все необходимые теоретические знания, но игнорируя при этом практические навыки. Кроме того, ни один из российских учебных центров не имеет официального статуса авторизованного учебного центра и соответственно не может предоставить обучение по программе авторизованных курсов.

Так можно сделать вывод, что курсы CompTIA можно использовать для подготовки к сертификации по подтверждению статуса начинающего специалиста в области безопасности или сетевых технологий.

Что касается компании EC-Council, то она настроена на обучение специалистов прикладного уровня и предлагает больший спектр курсов по безопасности – от защиты локальных рабочих станций до создания безопасного кода.

The International Council of Electronic Commerce Consultants (EC-Council) — профессиональная организация, созданная для поддержки компаний и индивидуальных предпринимателей в сфере электронной коммерции. Компания EC-Council не зависит от отдельных производителей и предлагает обучить и проверить знания кандидатов по всем сферам безопасности.

Курсы EC-Council предоставляют не только теоретическую подготовку, но и полезные практические навыки, а также редкое программное обеспечение для своих слушателей. К тому же EC-Council требует высокой квалификации от своих тренеров и периодически обновляет материалы курсов для повышения эффективности занятий.

Основными преимуществами обучающих программ от EC-Council является возможность применить теоретические навыки в лабораторной среде без вреда сетевой инфраструктуре организации. Кроме этого, каждому слушателю предоставляется возможность подтвердить полученные навыки, сдав экзамен по прослушанному курсу бесплатно.

Наиболее популярными являются курсы «Этичный хакинг и тестирование на проникновение» (Certified Ethical Hacker) и «Администратор сетевой безопасности» (EC-Council Network Security Administrator), позволяющие взглянуть на безопасность ИТ-инфраструктуры изнутри и снаружи.

Также весьма полезен курс «Сертифицированный пользователь безопасного компьютера» (Certified Secure Computer User), обучающий пользователя пресекать попытки применения к нему социальной инженерии и внедрения вредоносного кода на рабочую станцию.

Желающие навредить организации злоумышленники могут действовать как снаружи, так и изнутри. Для обеспечения безопасности организации нужно знать механизмы их действий более подробно.

Чтобы эффективно противодействовать злоумышленнику, желающему вторгнуться в вашу сеть, необходимо думать и рассуждать как злоумышленник, тогда можно будет предугадать вредоносные действия и противостоять вторжению. На курсе «Этичный хакинг и тестирование на проникновение» слушателям предлагают разобрать основные этапы подготовки и проведения атак на сети и системы. Подробно рассматриваются методы сбора информации о системе, сканирование портов для сетевого взаимодействия, обнаружение и перечисление доступных уязвимостей. Также рассмотрены способы взлома паролей, повышения привилегий, создания «черных выходов» (бэкдоров) и получения доступа к ресурсам.

Слушатели курса узнают, как можно обнаружить уязвимость системы и какие утилиты злоумышленники используют для проведения атак. При этом, набор всех необходимых утилит входит в комплект курса. Также слушатели познакомятся с приемами социальной инженерии, основными способами взлома систем семейства Windows и Linux, методами внедрения вредоносного кода в целевые системы и возможности обхода систем обнаружения вторжений (IDS).

В курсе, посвященном этичному хакингу, также рассмотрены моральные составляющие и правовые аспекты применения полученных на курсе знаний и навыков. В завершении курса «Этичный хакинг и тестирование на проникновение» слушателям предлагается лабораторная работа по тестированию на проникновение настроенной виртуальной среды.

Дополняющим курсом для «Этичного хакинга и тестирования на проникновение» будет курс «Администратор сетевой безопасности», где основной целью будет настройка параметров безопасности для противодействия вторжению.

Слушатели курса получат структурированное представление о работе сетевых служб и протоколов, познакомятся с системами обнаружения вторжений и общими рекомендациями по их настройке, научатся тестировать брандмауэр и устранять общие неисправности сети.

Кроме этого, слушатели узнают, как обеспечить безопасность при передаче электронной почты, установке VPN-соединения и взаимодействии с беспроводной сетью. Также в курсе рассматриваются темы общей настройки защищенной конфигурации операционных систем семейств Windows/Linux/RedHat, типовые настройки безопасности маршрутизаторов Cisco и обеспечение безопасности приложений.

Отдельными модулями рассматриваются темы обработки инцидентов, анализа журналов, восстановления систем после чрезвычайных ситуаций. По окончании обучения слушателям предлагают провести оценку сетевых уязвимостей виртуальной среды с помощью специализированных утилит, входящих в комплект курса.

Защита программных и аппаратных компонентов необходима для обеспечения безопасности, но недостаточна. Поэтому для рядовых пользователей компания EC-Council разработала курс «Сертифицированный пользователь безопасного компьютера», где рассмотрены основные причины взлома персональных компьютеров и электронной почты, основы антивирусной защиты и безопасного просмотра страниц в интернете, защита данных кредитных карт и взаимодействие с социальными сетями.

В курсе слушатели научатся распознавать атаки социальной инженерии, отслеживать активность антивирусных программ и настраивать безопасность мобильных устройств. Также пользователи узнают, как выбрать безопасное подключение к беспроводной сети, зачем использовать цифровую подпись и для чего выполнять резервное копирование данных.

По окончании обучения слушатели получают необходимые знания для противодействия типичным атакам, что позволит снизить влияние человеческого фактора на безопасность организации, а также по завершении программы выдается международный сертификат об успешном усвоении материалов курса.

Таким образом, основными программами от EC-Council можно решить вопрос накопления специфических знаний о безопасности ИТ-инфраструктуры. Более детальные настройки операционных систем можно найти в курсах по администрированию клиента или сервера Windows, курсах по RedHat или сетевому оборудованию Cisco, где более детально рассмотрены особенности обеспечения безопасности сетевой инфраструктуры.

С аппаратной точки зрения при настройке системы безопасности встают вопросы конфигурации конкретного сетевого оборудования, которые детально рассматриваются в вендорских курсах по теме безопасности. Для Cisco это, например, курсы Security, Firewall и IINS .

В курсах EC-Council описаны методы взлома систем. Целесообразно не только обезопасить себя от подобных атак, но и оперативно контролировать попытки взлома систем безопасности. Для этого применяют средства IPS/IDS или WIPS/WIDS для беспроводных систем.

Спектр современных сетевых устройств включает множество функциональных компонентов, в целом обеспечивающих сквозную защиту сети от вторжений. Для правильной организации инфраструктуры сети разработаны курсы Cisco DESIGN.

CSCU

- ✓ Как работать без риска для компании?
- ✓ Как уберечь свои и корпоративные данные?
- ✓ Как обеспечить защиту пользователя?
- ✓ Как противодействовать социальной инженерии?

Повседневная работа

DESIGN

- ✓ Как повысить производительность сети?
- ✓ Как сделать сеть безопасной и управляемой?
- ✓ Как обеспечить отказоустойчивость сети?
- ✓ Как правильно спроектировать сеть?
- ✓ Как найти баланс между ценой и качеством?

Архитектура систем

ENSA

- ✓ Как защитить корпоративные ресурсы?
- ✓ Как управлять системой безопасности?
- ✓ Как учесть все возможные риски?
- ✓ Как провести аудит системы безопасности?

Настройка систем

IUWNE IAUWS

- ✓ Что дают беспроводные сети?
- ✓ Как правильно настроить сеть?
- ✓ Как можно управлять сетью?
- ✓ Как защитить данные в сети?
- ✓ Как обеспечить отказоустойчивость?

Беспроводные системы

CEH

- ✓ Как мыслит хакер, проникая в вашу сеть?
- ✓ Как организуется атака?
- ✓ Какие средства использует хакер?
- ✓ Какова методика проникновения?
- ✓ Как протестировать свою сеть?

Тестирование на проникновение

EC-Council

IPS

- ✓ Как можно защитить ресурсы сети?
- ✓ Как выявить факт атаки на сеть?
- ✓ Как вычислить злоумышленников?
- ✓ Как настроить аппаратные средства безопасности?
- ✓ Как предотвратить проникновение?

Предотвращение проникновений

Сражаясь с тем, кто умеет обороняться, противник не знает, где ему нападать

Курсы EC-Council

Программа обучения EC-Council готовит специалистов для противодействия вторжениям. В зависимости от требуемого уровня и специфики деятельности, могут быть выбраны различные курсы. Каждый из курсов ориентирован на решение определенных задач, и наиболее востребованными курсами являются:

- ✓ CEH (Certified Ethical Hacker);
- ✓ ENSA (EC-Council Network Security Administrator);
- ✓ CSCU (Certified Secure Computer User).

Certified Ethical Hacker – это квалифицированный профессионал, который знает и понимает, как найти недостатки и слабые места системы безопасности **снаружи**, используя подходы, знания и инструменты хакеров-злоумышленников.

EC-Council Network Security Administrator - это профессионал, который знает и понимает, как найти недостатки и слабые места системы **изнутри,** как укрепить систему безопасности имеющимися средствами и противостоять вторжению.

Certified Secure Computer User - это квалифицированный пользователь, **умеющий пресекать** попытки применения к нему социальной инженерии и внедрения вредоносного кода на рабочую станцию.

В рамках курса CEH каждый слушатель обеспечивается огромным количеством разнообразных современных инструментов для взлома систем, получает доступ к системе Frankenstein, значительно упрощающей работу с этими инструментами. Помимо этого, на занятиях используется специально подготовленная лабораторная среда, где студенты могут практиковать свои навыки в виртуальной среде в реальном времени.

Слушатели знакомятся с примерами и приемами социальной инженерии, основными способами взлома систем семейства Windows и Linux, методами внедрения вредоносного кода в целевые системы и возможности обхода систем обнаружения вторжений.

Каждым курсом предусмотрены лабораторные работы, специально разработанные для наилучшего усвоения материала.

По окончании каждого курса слушатели получают международный **номерной** сертификат об успешном усвоении программы.

CEH

Certified Ethical Hacker

Обзор курса

Цель курса – дать слушателям знания и навыки для формирования системного подхода к обеспечению компьютерной безопасности, научить методам проверки безопасности различных узлов компьютерной сети и познакомить слушателей с инструментарием злоумышленников, с их преимуществами и ограничениями.

Слушателям предоставляется фирменное учебное пособие и прочие материалы, необходимые для обучения.

По окончании курса вы сможете:

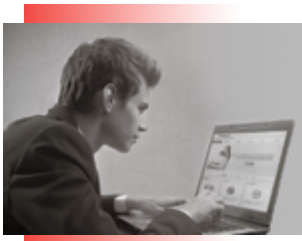
- ☑ понимать взаимосвязь компонентов безопасности сети, сферу ответственности и влияния каждого из узлов;
- ☑ знать и управлять уязвимыми местами сети;
- ☑ использовать мониторинг и самостоятельно обнаруживать уязвимости;
- ☑ работать с инструментами взлома сетей и систем;
- ☑ знать хакерские уловки для проникновения в системы и сети;
- ☑ проводить тестирование любых компонентов сети на предмет взлома;
- ☑ классифицировать рабочие станции по степени риска проведения атаки;
- ☑ понимать ход мыслей злоумышленника;
- ☑ оценить масштаб потенциально возможных атак;
- ☑ противодействовать несанкционированному сбору информации о сети организации;
- ☑ понимать стратегию злоумышленника;
- ☑ определять атаку на основе социальной инженерии;
- ☑ изучить методы взлома беспроводной сети;
- ☑ определить наиболее уязвимые места мобильных платформ;
- ☑ противодействовать криптографическим атакам;
- ☑ понимать процесс вторжения в систему;
- ☑ проводить аудит систем безопасности;
- ☑ противодействовать вторжению.

Содержание курса

- ○ Введение в этичный хакинг
- ○ Предварительный сбор информации о цели
- ○ Сканирование сети
- ○ Инвентаризация ресурсов
- ○ Хакинг системы
- ○ Трояны и бэкдоры
- ○ Вирусы и черви
- ○ Снифферы
- ○ Социальная инженерия
- ○ Отказ в обслуживании
- ○ Перехват сеанса
- ○ Хакинг веб-серверов
- ○ Хакинг веб-приложений
- ○ SQL инъекции
- ○ Хакинг беспроводных сетей
- ○ Хакинг мобильных платформ
- ○ Обход систем обнаружения вторжений, брандмауэры и Honey Pot
- ○ Переполнение буфера
- ○ Криптография
- ○ Тестирование на проникновение

Дополнительная информация

- ✓ Экзамен: **312-50**
- ✓ Число вопросов: **150**
- ✓ Проходной балл: **70%**
- ✓ Длительность: **4 часа**



EC-Council Network Security Administrator

ENSA

Обзор курса

Цель курса – предоставить слушателям расширенные знания и навыки, необходимые для анализа внутренних и внешних угроз безопасности в отношении сетей, разработки политики безопасности для защиты информации организации. Курс рассматривает вопросы оценки локальной сети и безопасности подключения к Интернету, а также дизайн сети, реализацию успешной политики безопасности и стратегии использования брандмауэра, выявление системных и сетевых уязвимостей и защиты от них. Курс ENSA направлен на обеспечение защиты от атак на систему безопасности, в то время как курс CEH рассматривает методы осуществления этих атак.

По окончании курса вы сможете:

- ☑ анализировать сетевые протоколы передачи;
- ☑ управлять разными уровнями безопасности организации;
- ☑ разбираться в различных стандартах безопасности;
- ☑ понимать концепции работы IDS и IPS;
- ☑ разбираться в возможностях настройки безопасности сетевого оборудования;
- ☑ настраивать брандмауэры, системы обнаружения вторжений и AV системы;
- ☑ разрабатывать эффективные политики безопасности в компании;
- ☑ обеспечить безопасность работы приложений и передачи эл.почты;
- ☑ обеспечивать отказоустойчивость системы;
- ☑ организовать процесс обработки инцидентов;
- ☑ реализовать оценку уязвимостей.

Содержание курса

- ○ Основы компьютерных сетей
- ○ Сетевые протоколы
- ○ Анализ протоколов TCP / IP
- ○ Повышение уровня физической безопасности
- ○ Безопасность сети
- ○ Стандарты безопасности организации
- ○ Стандарты безопасности
- ○ Политика безопасности
- ○ Стандарты IEEE
- ○ Угрозы безопасности сети
- ○ Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS)
- ○ Брандмауэры (Firewalls)
- ○ Фильтрация пакетов и прокси-серверы
- ○ Узел-бастионы (Bastion Host) и ловушки (Honeypot)
- ○ Обеспечение безопасности модемов
- ○ Устранение неисправностей сети
- ○ Повышение уровня защиты маршрутизаторов
- ○ Фиксация настроек операционной системы
- ○ Управление заплатками
- ○ Анализ журнала
- ○ Безопасность приложений
- ○ Веб-безопасность
- ○ Безопасность электронной почты
- ○ Аутентификация: Шифрование, криптография и цифровые подписи
- ○ Virtual Private Networks
- ○ Безопасность беспроводных сетей
- ○ Обеспечение отказоустойчивости
- ○ Обработка инцидентов
- ○ Восстановление после чрезвычайных ситуаций и планирование
- ○ Оценка сетевой уязвимости

Дополнительная информация

- ✓ Экзамен: **312-38**
- ✓ Число вопросов: **50**
- ✓ Проходной балл: **70%**
- ✓ Длительность: **2 часа**

CSCU

Certified Secure Computer User

Обзор курса

Цель курса – предоставить слушателям расширенные знания и навыки, необходимые для защиты своих компьютеров, учетных записей, конфиденциальных данных и мобильных устройств от угроз в среде ИТ. Курс погружает слушателей в интерактивную среду, где можно приобрести глубокое понимание различных составляющих компьютерной безопасности и сетевых угроз. В курсе рассмотрены способы кражи личных данных, мошенничество с кредитными картами, онлайн-банкинг фишинг, вирусы и бэкдоры, подмена электронной почты, потеря конфиденциальной информации, хакерские атаки и социальная инженерия. Данный курс посвящает пользователей в основы обеспечения информационной безопасности и позволяет повысить общий уровень защиты организации.

По окончании курса вы сможете:

- ☑ знать и понимать основы компьютерной безопасности;
- ☑ поддерживать безопасность операционных систем;
- ☑ защищать операционную систему с помощью антивируса;
- ☑ шифровать конфиденциальные данные;
- ☑ работать с резервными копиями данных и восстановлением системы после отказов;
- ☑ безопасно работать в Internet;
- ☑ работать с безопасными сетевыми подключениями;
- ☑ обеспечить безопасность передачи файлов online;
- ☑ обеспечивать безопасность передачи эл.почты;
- ☑ противодействовать социальной инженерии и распознавать кражу конфиденциальной информации;
- ☑ безопасно посещать ресурсы социальных сетей;
- ☑ понимать концепции информационной безопасности и законодательную основу обеспечения безопасности;
- ☑ поддерживать безопасность мобильных устройств.

Содержание курса

- ○ Основы безопасности
- ○ Обеспечение безопасности операционных систем
- ○ Защита системы с помощью антивирусов
- ○ Шифрование данных
- ○ Резервное копирование и аварийное восстановление
- ○ Безопасность в Интернете
- ○ Обеспечение безопасности сетевых подключений
- ○ Организация безопасности передачи данных по сети
- ○ Защита сообщений электронной почты
- ○ Социальная инженерия и кражи личных данных
- ○ Безопасность в социальных сетях
- ○ Информационная безопасность и соблюдение законов
- ○ Обеспечение безопасности мобильных устройств

Дополнительная информация

- ✓ Экзамен: **112-12**
- ✓ Число вопросов: **50**
- ✓ Проходной балл: **70%**
- ✓ Длительность: **2 часа**

Безопасность - это процесс, а не результат...

Курсы Cisco

Программа обучения Cisco готовит специалистов высшего технического уровня, способных, в том числе, обеспечить эффективное и безопасное функционирование сети масштаба корпорации. Спектр направлений обучения и курсов Cisco велик, однако с точки зрения обеспечения безопасности наиболее полезными будут курсы следующих направлений:

- ✓ проектирование (Design);
- ✓ беспроводные сети (Wireless);
- ✓ безопасность (Security).

Проектирование - специалисты, обучающиеся по этому направлению, получают системное понимание того, какие функциональные возможности предоставляют продукты и технологии Cisco, из каких блоков состоит структура защищенной сети, как шаг за шагом укреплять безопасность корпоративной сети.

Основополагающим курсом направления является курс DESGN.

Беспроводные сети - специалисты, обучающиеся по этому направлению, получают знания в области проектирования, установки и безопасной эксплуатации беспроводных сетей стандарта 802.11.

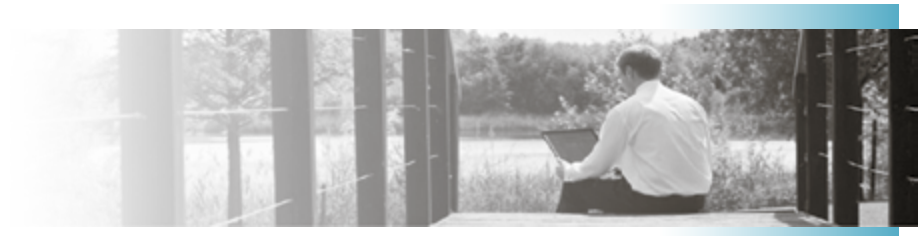
Программа охватывает множество аспектов беспроводных технологий, однако с точки зрения обеспечения безопасности, наиболее полезными будут курсы IUWNE и IAUWS.

Безопасность - курсы, представленные компанией Cisco в рамках этого направления полностью посвящены ответам на вопросы обеспечения безопасности сетей. С их помощью вы совершенствуете ваши навыки и умения в работе с различным современным оборудованием, технологиями, протоколами безопасности.

Актуальными курсами по безопасности являются такие, как IINS, FIREWALL, VPN, IPS, SECURE.

В состав каждого курса входят лабораторные работы, помогающие проверить и закрепить полученные знания. Работы выполняются на реальном оборудовании в сертифицированной лабораторной среде.

По окончании курсов слушателям выдаются **номерные** сертификаты международного образца. При прохождении программы курсов и после сдачи серии экзаменов слушателю может быть присвоено звание сертифицированного специалиста, профессионала или эксперта.



DESGN

Designing for Cisco Internetwork Solutions

Обзор курса

Курс позволит слушателям выявлять требования заказчика к распределенным сетям, вырабатывать решения по реализации этих требований с учетом различных условий и ограничений, проводить проектирование сетей, обеспечивающих заданные характеристики.

Основная цель курса – научить слушателя проводить полный цикл обследования, анализа, проектирования распределенных сетей для заказчиков, применяя эффективные методики проектирования и используя современные сетевые технологии.

По окончании курса вы сможете:

- ☑ понимать методологию проектирования и создания сетей;
- ☑ описывать способы структурирования сетей и этапы проектирования, базирующиеся на принципах Cisco Network Architectures for the Enterprise;
- ☑ проектировать комплекс сетей предприятия, предлагать решения для центров обработки данных, оценивать целесообразность виртуализации;
- ☑ проектировать подключения предприятия к внешним сетям и организовывать сети филиалов;
- ☑ разрабатывать схему сетевой адресации и выбирать эффективные протоколы маршрутизации для спроектированной сети;
- ☑ вырабатывать решения по обеспечению безопасности сети;
- ☑ оценивать целесообразность использования технологий передачи голосовых и видеоданных по сети предприятия;
- ☑ оценивать целесообразность использования в составе сети предприятия технологий беспроводной передачи данных.

Содержание курса

- ○ Обзор методологии проектирования сетей
  - ● Учебный пример 1-1. Модернизация сети госпиталя
- ○ Структурирование и модульность в сети
  - ● Учебный пример 2-1. Структурирование сети госпиталя
- ○ Проектирование магистральных сетей и сетей центров обработки данных
  - ● Учебный пример 3-1. Проектирование магистральной сети госпиталя
- ○ Проектирование удаленных соединений
  - ● Учебный пример 4-1. Проектирование WAN сети госпиталя ACMC
- ○ Разработка сетевой IP адресации и выбор протоколов маршрутизации
  - ● Учебный пример 5-1. Проектирование сетевой адресации и выбор протоколов маршрутизации для госпиталя
- ○ Выработка решений по сетевой безопасности
  - ● Учебный пример 6-1. Проектирование безопасности для ACMC
- ○ Выявление потребности и особенностей передачи в сети голосовых и видео данных
  - ● Учебный пример 7-1. Особенности развертывания сетей передачи голоса
- ○ Выявление потребности и особенностей применения в сети беспроводных технологий
  - ● Учебный пример 8-1. Особенности внедрения беспроводных сетей

Дополнительная информация

По направлению повышения квалификации в области проектирования, кроме курса DESGN, рекомендуется прослушать курс ARCH «Проектирование архитектуры сетевых служб Cisco»

- ✓ Экзамен: **640-864**
- ✓ Число вопросов: **50-60**
- ✓ Длительность: **75 мин.**

IUWNE

Implementing Cisco Unified Wireless Networking Essentials

Обзор курса

Цель курса – предоставить слушателю сведения и навыки практической работы в области проектирования, установки, настройки, обслуживания и поиска неисправностей беспроводных сетей малого, среднего и корпоративного масштаба.

Объем курса предусматривает предоставление начальных сведений и не акцентирует внимание на расширенных возможностях решений Cisco WLAN.

По окончании курса вы сможете:

☑ объяснять принципы работы беспроводных сетей;
☑ устанавливать унифицированные беспроводные сети Cisco;
☑ осуществлять настройку типовых клиентов WLAN средствами операционной системы или специальных утилит;
☑ настраивать безопасность беспроводных сетей;
☑ управлять WLAN сетями при помощи программного пакета Cisco WCS;
☑ осуществлять эксплуатационную поддержку и поиск неисправностей в сетях WLAN.

Содержание курса

○ Основы беспроводных сетей
  ● Лабораторная работа 1-1: Знакомство с антеннами и зонами охвата
  ● Лабораторная работа 1-2: Организация сетей IBSS и анализ коммуникации
○ Основы построения WLAN Cisco
  ● Лабораторная работа 2-1: Настройка контроллера Cisco 2504
  ● Лабораторная работа 2-2: Восстановление конфигурации автономного режима на точке доступа, работающей под управлением контроллера
○ Беспроводные клиентские устройства
  ● Лабораторная работа 3-1: Настройка мобильных клиентов Cisco AnyConnect
  ● Лабораторная работа 3-2: Исследование подключений и роуминга
○ Безопасность беспроводных локальных сетей
  ● Лабораторная работа 4-1: Настройка PSK аутентификации на контроллере
  ● Лабораторная работа 4-2: PSK аутентификация на автономной точке
  ● Лабораторная работа 4-3: Настройка EAP-FAST; Аутентификации с WPA
  ● Лабораторная работа 4-4: Настройка аутентификации 802.1Q
○ Основы Cisco WCS
  ● Лабораторная работа 5-1: Настройка контроллеров и точек беспроводного доступа при помощи Cisco WCS
  ● Лабораторная работа 5-2: Работа с Cisco WCS
  ● Лабораторная работа 5-3: Мониторинг сети и захват сторонних устройств
○ Поддержка беспроводных сетей и устранение неисправностей
  ● Лабораторная работа 6-1: Резервирование конфигурационных файлов контроллеров Cisco WLC
  ● Лабораторная работа 6-2: Поиск и устранение неисправностей
  ● Лабораторная работа 6-3: Поиск и устранение неисправностей при помощи сниффера Wireshark и преобразование автономной точки в режим управления контроллером.

Дополнительная информация

Данный курс является базовым в линейке курсов Cisco, посвященных беспроводным сетям.

✓ Экзамен: **640-722**
✓ Число вопросов: **75-85**
✓ Длительность: **90 мин.**

IAUWS

Implementing Advanced Cisco Unified Wireless Security

Обзор курса

Цель курса – предоставить слушателям знания и практические навыки по обеспечению защиты беспроводных сетей от различных угроз средствами соответствующих политик безопасности, применения проверенных решений, аудита соответствия настроек компонентов системы современным стандартам безопасности.

По окончании курса вы сможете:

- ☑ интерпретировать корпоративные и законодательные требования к обеспечению безопасности и обеспечивать соответствующий уровень защиты сети;
- ☑ обеспечивать безопасность на клиентских устройствах;
- ☑ проектировать и предоставлять услуги гостевого доступа на WLAN контроллерах;
- ☑ проектировать и интегрировать беспроводные сети с устройствами Cisco NAC;
- ☑ внедрять сервисы защищенных соединений на контроллерах WLAN;
- ☑ использовать встроенные средства безопасности WLAN контроллеров, а также интегрировать их в комплексные системы безопасности для изоляции и снижения угроз безопасности WLAN.

Содержание курса

- ○ Корпоративные и законодательные требования к обеспечению безопасности
  - ● Лабораторная работа 1-1: Сегментирование трафика
  - ● Лабораторная работа 1-2: Настройка административной безопасности
- ○ Защита клиентских устройств
  - ● Лабораторная работа 2-1: Настройка локальной аутентификации на автономной точке и на WLAN контроллере
  - ● Лабораторная работа 2-2: Настройка сервиса сертификатов и защищенной аутентификации
  - ● Лабораторная работа 2-3: Настройка H-REAP для отработки сбоев в сети
  - ● Лабораторная работа 2-4: Настройка Cisco OEAP
  - ● Лабораторная работа 2-5: Внедрение списков контроля доступа
  - ● Лабораторная работа 2-6: Внедрение IBNS
  - ● Лабораторная работа 2-7: Диагностика проблем EAP аутентификации
- ○ Проектирование и обеспечение услуги гостевого доступа
  - ● Лабораторная работа 3-1: Настройка гостевого доступа для WLAN
  - ● Лабораторная работа 3-2: Настройка контроллера на аутентификацию с использованием гостевого сервера NAC
  - ● Лабораторная работа: Диагностика неисправностей гостевого доступа
- ○ Проектирование и интеграция WLAN-сетей с устройствами Cisco NAC
- ○ Внутренние и встроенные средства снижения уязвимости
  - ● Лабораторная работа 5-1: Управление несанкционированными точками беспроводного доступа
  - ● Лабораторная работа 5-2: Настройка защиты кадров управления (MFP)
  - ● Лабораторная работа 5-3: Настройка wIPS

Дополнительная информация

В области беспроводных сетей, рекомендуется прослушать комплекс курсов, включая дополнительно CUWSS, IUWVN, IUWMS. В них рассматриваются вопросы радиочастотного обследования объектов, развертывание беспроводных голосовых сетей и мобильных сервисов.

- ✓ Экзамен: **642-737**
- ✓ Число вопросов: **50-60**
- ✓ Длительность: **90 мин.**

Implementing Cisco Intrusion Prevention System

IPS

Обзор курса

Основная цель курса – научить слушателя внедрять в сетевую инфраструктуру системы предотвращения атак, как в виде независимых устройств, так и в виде специализированных модулей к устройствам Cisco.

По окончании курса вы сможете:

- ☑ оценивать продукты и архитектуру развертывания продуктовой линейки IPS;
- ☑ выполнять начальную настройку сенсоров Cisco IPS;
- ☑ настраивать первоначальную политику безопасности, используя сенсоры Cisco IPS, в соответствии с политиками и требованиями безопасности конкретной сети;
- ☑ оптимизировать политики сенсора для корректного реагирования при работе в конкретной сетевой инфраструктуре;
- ☑ настраивать мониторинг и управление событиями сенсора;
- ☑ оптимизировать характеристики сенсора для повышения производительности и отказоустойчивости;
- ☑ выполнять настройку и поддержку сетевых IPS модулей для различных устройств Cisco.

Содержание курса

- ○ Обзор технологий предотвращения вторжений и устройств Cisco IPS
- ○ Установка и поддержка сенсоров Cisco IPS
  - ● Лабораторная работа. Размещение сенсора Cisco IPS в сети
- ○ Применение политик сенсора Cisco IPS
  - ● Лабораторная работа. Настройка сенсора Cisco IPS
  - ● Лабораторная работа. Базовая настройка проверки трафика
- ○ Оптимизация работы сенсора в условиях конкретной сети
  - ● Лабораторная работа. Настройка обнаружения аномального трафика
  - ● Лабораторная работа. Настройка пользовательских Cisco IPS сигнатур
  - ● Лабораторная работа. Настройка ложных срабатываний и пропуска атаки
- ○ Средства управления и анализа событий сенсора
  - ● Лабораторная работа. Улучшение работы обнаружений и оповещений атак
  - ● Лабораторная работа. Использование Cisco IME
  - ● Лабораторная работа. Использование Cisco IPS and Security Intelligence Web Resources
- ○ Внедрение решений по виртуализации, обеспечению высокой доступности и максимальной производительности
- ○ Настройка и поддержка модулей для ASA, Catalyst 6500, маршрутизаторов ISR
  - ● Лабораторная работа. Настройка виртуальных сенсоров Cisco IPS

Дополнительная информация

В области обеспечения безопасности Cisco учебный центр Эврика представляет полный спектр курсов, включающий в том числе IINS, SECURE, FIREWALL, VPN, CANAC.

- ✓ Экзамен: **642-627**
- ✓ Число вопросов: **60-70**
- ✓ Длительность: **90 мин.**

ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА
КОМИТЕТ ПО ОБРАЗОВАНИЮ
наименование лицензирующего органа

ЛИЦЕНЗИЯ

на право ведения образовательной деятельности

Регистрационный № 781 «09» декабря 2011 г.

Настоящая лицензия выдана

Негосударственному образовательному учреждению

дополнительного образования «Учебный центр «Эврика»

НОУДО «Учебный центр «Эврика»

частное учреждение
полное и сокращенное (при наличии) наименования и организационно-правовая форма лицензиата в соответствии с его уставом

191023, Россия, Санкт-Петербург, ул. Гороховая, д. 32, литер А, пом. 3-Н
место нахождения лицензиата

1027809229502
основной государственный регистрационный номер записи о государственной регистрации юридического лица

7825491088
идентификационный номер налогоплательщика

на право ведения образовательной деятельности в соответствии с приложением (приложениями).

Срок действия лицензии по **бессрочно** «____» _____ 20___ г.

Лицензия без приложения (приложений) недействительна.

Председатель Комитета **Иванова Ольга Владимировна**
руководитель лицензирующего органа — подпись — фамилия, имя, отчество

М. П.

78 № 001127

ЭВРИКА

Выбери путь
Будь в безопасности

196084, Санкт-Петербург,
Московский пр., 118

+7 (812) 718-61-84