Основы кибербезопасности 1.0. Область применения и содержание

Последнее обновление 3 января 2018 г.

Целевая аудитория

Курс *«Основы кибербезопасности 1.0»* предназначен для студентов, заинтересованных в более углубленном изучении кибербезопасности. В этом подготовительном курсе обзорно предоставлена сфера кибербезопасности. В учебном курсе изучаются характеристики киберпреступников и тактики, используемые ими. Кроме того, в нем рассказывается о технологиях, средствах и процедурах, которые специалисты по кибербезопасности используют для борьбы с киберпреступностью. Эта программа подходит для учащихся с самым разным уровнем образования, которые обучаются в различных учебных заведениях, среди которых средняя школа (на базе как девяти, так и одиннадцати лет), университеты, колледжи, профессиональные и технические училища.

Предварительная подготовка

Для приобретения необходимых навыков студенты должны быть знакомы с содержанием предварительного курса:

- Введение в кибербезопасность 2.0

Цели сертификации

Для этого курса целевые сертификации не предусмотрены

Описание учебного плана

В курсе имеется много функций, помогающих учащимся понять следующие концепции.

- Насыщенное мультимедийное содержание, включая интерактивные упражнения, видео, игры и контрольные работы, обеспечивает разные стили обучения, стимулирует интерес к учебе и улучшает запоминание материала
- Практические лабораторные работы и обучающие упражнения на основе моделирования с использованием программы Packet Tracer способствуют развитию у учащихся критического мышления и навыков решения сложных проблем
- Новаторская система аттестаций обеспечивает немедленную обратную связь для оценки знаний и приобретенных навыков.
- Технические принципы объясняются языком, который доступен студентам всех уровней, а встроенные интерактивные задания облегчают понимание содержимого и способствуют укреплению знакомства с материалом
- Учебный план побуждает учащихся задуматься о дополнительном образовании в сфере ИТ, но в нем также придается особое значение применению навыков и практическому опыту

Операции Cisco Packet Tracer разработаны для использования с Packet Tracer версии не ниже 6.3.

Цели учебного курса

Курс *«Основы кибербезопасности 1.0»* обеспечивает получение базовых знаний и навыков, охватывающих все области кибербезопасности — информационную безопасность, безопасность систем и сетей, безопасность мобильных устройств, физическую безопасность, этические и правовые требования, технологии и методы защиты и минимизации последствий в ходе обеспечения информационной безопасности бизнеса.

После прохождения курса *Основы кибербезопасности 1.0* учащиеся смогут выполнять следующие задачи.

- назвать отличительные черты преступников в сфере кибербезопасности и тех, кто им противостоит;
- объяснить, как принципы конфиденциальности, целостности и доступности соотносятся с состояниями данных и средствами противодействия угрозам безопасности;
- описать тактику, методы и процедуры, используемые киберпреступниками;
- перечислить способы защиты конфиденциальности с помощью технологий, продуктов и процедур;
- перечислить способы обеспечения целостности данных с помощью технологий, продуктов и процедур;
- перечислить способы обеспечения высокой доступности с помощью технологий, продуктов и процедур;
- Объясните, как профессионалы по кибербезопасности используют технологии, процессы и процедуры для защиты всех компонентов сетевой инфраструктуры.
- Объясните цель законов, относящихся к кибербезопасности.

Минимальные системные требования

Чтобы процесс обучения каждого учащегося был оптимальным, рекомендуется организовать в классе от 12 до 15 рабочих мест и обеспечить отдельный компьютер каждому учащемуся. На одном лабораторном компьютере не должно совместно работать больше двух учащихся при выполнении лабораторных работ. Для некоторых лабораторных работ потребуется, чтобы компьютеры учащихся были подключены к локальной сети.

Требования к оборудованию лабораторных ПК

- Компьютер с ОЗУ не менее 2 ГБ и 8 ГБ свободного дискового пространства
- Высокоскоростной доступ в Интернет для загрузки приложения Oracle VirtualBox и файла образа виртуальной машины.

Обзор программы

Курс *Основы кибербезопасности 1.0* дает учащимся возможность:

- познакомиться с миром кибербезопасности и узнать о мотивации киберпреступников и специалистов по кибербезопасности;
- научиться определять кибератаки и их признаки, процессы и контрмеры информационной безопасности;
- получить фундаментальные знания в различных областях безопасности;
- приобрести навыки по управлению безопасностью, использованию средств контроля, защиты и технологий минимизации последствий;
- узнать об этических требованиях и законах в области информационной безопасности и методах разработки политик безопасности;
- узнать о функциях специалистов по кибербезопасности и карьерных возможностях.

Описание курса

Таблица 1. Описание курса «Основы кибербезопасности 1.0»

Глава/Раздел	Цели/задачи
Глава 1. Кибербезопасность. Мир мастеров, героев и преступников	**назвать отличительные черты преступников в сфере кибербезопасности и тех, кто им противостоит;**
1.1 Мир кибербезопасности	Опишите общие черты мира кибербезопасности.
1.2 Киберпреступники против специалистов по кибербезопасности	Покажите различия между киберпреступниками и теми, кто им противостоит.
1.3 Угрозы благосостоянию	Расскажите, как киберугрозы затрагивают людей, предприятия и организации.
1.4 Темная сторона мира кибербезопасности	Опишите факторы, которые ведут к распространению и росту киберпреступности.
1.5 Обучение дополнительных специалистов	Расскажите об организациях и инициативах, направленных на подготовку большего числа специалистов по кибербезопасности.
Глава 2. Куб кибербезопасности	**объяснить, как принципы конфиденциальности, целостности и доступности соотносятся с состояниями данных и средствами противодействия угрозам безопасности;**
2.1 Куб кибербезопасности	Описываются три грани куба МакКамбера.
2.2 Триада «КЦД»	Опишите принципы конфиденциальности, целостности и доступности.
2.3 Состояния данных	Опишите различия трех состояний данных.
2.4 Средства противодействия угрозам безопасности	Сравните типы средств противодействия угрозам безопасности.
2.5 Архитектура управления безопасностью ИТ-среды	Опишите модель кибербезопасности в соответствии с ISO.
Глава 3. Угрозы кибербезопасности, уязвимости системы кибербезопасности и атаки на нее	**Опишите тактику, методы и процедуры, используемые киберпреступниками.**
3.1 Вредоносное ПО и вредоносный код	Рассмотрите различные типы вредоносного ПО и вредоносного кода.
3.2 Обман	Сравните различные методы, используемые в социальной инженерии.
3.3 Атаки	Сравните различные типы кибератак.
Глава 4. Способы защиты секретной информации	**перечислить способы защиты конфиденциальности с помощью технологий, продуктов и процедур;**
4.1 Криптография	Объясните, как методы шифрования защищают конфиденциальность данных.
4.2 Средства контроля доступа	Опишите, каким образом методы контроля доступа защищают конфиденциальные данные.
4.3 Сокрытие данных	Опишите концепцию сокрытия данных.

Глава 5. Искусство обеспечения целостности данных	**перечислить способы обеспечения целостности данных с помощью технологий, продуктов и процедур;**
5.1 Виды средств контроля целостности данных	Расскажите о процессах, используемых для обеспечения целостности.
5.2 Цифровые подписи	Объясните назначение цифровых подписей.
5.3 Сертификаты	Объясните назначение цифровых сертификатов.
5.4 Обеспечение целостности баз данных	Объясните необходимость в обеспечении целостности баз данных.
Глава 6. Область применения концепции «пять девяток»	**Перечислите способы обеспечения высокой доступности с помощью технологий, продуктов и процедур.**
6.1 Высокая доступность	Объясните понятие высокой доступности.
6.2 Меры по повышению доступности	Объясните повышение доступности с помощью мер по обеспечению высокой доступности.
6.3 Реагирование на инциденты	Объясните достижение высокой доступности с помощью плана реагирования на инциденты.
6.4 Аварийное восстановление	Объясните роль плана аварийного восстановления в достижении высокой доступности.
Глава 7. Возведение укреплений	**Объясните, как профессионалы по кибербезопасности используют технологии, процессы и процедуры для защиты всех компонентов сетевой инфраструктуры.**
7.1 Защита систем и устройств	Объясните, каким образом процессы и процедуры защищают систему.
7.2 Повышение надежности сервера	Поясните способы защиты серверов в сетевой инфраструктуре.
7.3 Повышение надежности сетевой инфраструктуры	Поясните способы внедрения мер обеспечения безопасности для защиты сетевых устройств.
7.4 Физическая безопасность и безопасность условий работы	Опишите, как внедрение физических средств обеспечения безопасности влияет на защиту сетевого оборудования.
Глава 8. Вступление в профессиональное сообщество специалистов по кибербезопасности	**Объясните цель законов, относящихся к кибербезопасности.**
8.1 Уровни обеспечения кибербезопасности	Опишите уровни обеспечения кибербезопасности в рамках триады «конфиденциальность, целостность, доступность».
8.2 Понимание ответственности	Поясните этические ценности в сфере кибербезопасности, и как ими руководствоваться.
8.3 Следующий шаг	Расскажите, какие действия нужно выполнить в дальнейшем для того, чтобы стать специалистом по кибербезопасности