АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ДВ.2.2 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Автор:

Преподаватель В.А. Карпов

Код и наименование направления подготовки, профиля:

43.03.01 Сервис, «Сервис транспортных средств»

Квалификация (степень) выпускника:

Бакалавр

Цель освоения дисциплины:

Сформировать компетенцию в области комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов.

План курса:

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Раздел 1	Концепция информационной безопасности.	Актуальность информационной безопасности. Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Лицензирование и сертификация в области защиты информации. Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования. Основные нормативные руководящие документы. Международные стандарты информационного обмена. Критерии безопасности компьютерных систем. «Оранжевая книга». Руководящие документы Гостехкомиссии.
Раздел 2	Угрозы информации.	Информационная безопасность сетей. Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ. Способы совершения компьютерных преступлений. Уязвимость сети Интернет. Пользователи и злоумышленники в Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
Раздел 3	Виды возможных нарушений информационной системы	Компьютерные преступления. Классификация компьютерных преступлений. Виды противников или «нарушителей». Вредоносные программы. Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Вирусы. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.
Раздел 4	Информационная безопасность информационных систем.	Теория информационной безопасности информационных систем. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Криптографические способы защиты информации. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Организация информационной безопасности компании. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.
Раздел 5	Методы и средства защиты компьютерной информации.	Обеспечения информационной безопасности. Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Контроль доступа к информации. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Методы и средства защиты информации. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Антивирусное ПО. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

Формы текущего контроля и промежуточной аттестации:

В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении занятий лекционного типа:
метод проблемного изложения, фронтальные и комбинированные опросы;

– при проведении занятий семинарского типа:

- тестирование;
- реферат.

Экзамены проводятся в письменной форме с решением практических задач.

Основная литература:

1.Артемов А.В. Информационная безопасность. МАБИВ, 2014. http://www.iprbookshop.ru/33430

2. Милославская Н.Г. Управление рисками информационной безопасности. Горячая линия, 2012. http://www.iprbookshop.ru/12060