

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ДОНЕЦКАЯ АКАДЕМИЯ УПРАВЛЕНИЯ И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ГЛАВЕ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ"

Факультет Государственной службы и управления
Кафедра Информационных технологий

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
"Защита информации в корпоративных информационных системах"

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины – формирование компетенций магистров в области аудита состояния информационной безопасности корпоративных информационных систем.

2. УЧЕБНЫЕ ЗАДАЧИ ДИСЦИПЛИНЫ

Задачи учебной дисциплины:

- ознакомиться с законодательным уровнем обеспечения информационной безопасности;
- изучить административный уровень информационной безопасности;
- научиться использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации ИС.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Цикл (раздел) ОПОП ВО: Б1.В.02.01

1.3.1. Дисциплина "Защита информации в корпоративных информационных системах" опирается

1.3.2. Дисциплина "Защита информации в корпоративных информационных системах" выступает

Преддипломная практика

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-6, ПК-9, ПК-10, ПК-21, ПК-28

В результате освоения дисциплины обучающийся должен:

3.1 | Знать:

методы и средства защиты от вредоносных программ

основные понятия защиты информации

основные методы, средства и стандарты информатики для решения прикладных задач, понимать их назначение и особенности

основные понятия прикладных и информационных процессов

основные понятия защиты информации

3.2 | Уметь:

использовать типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду

анализировать угрозы информационной безопасности в корпоративных системах

проводить маркетинговый анализ ИКТ и вычислительного оборудования

проводить реинжиниринг прикладных и информационных процессов

анализировать угрозы информационной безопасности в корпоративных системах

3.3 | Владеть:

навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях

навыками анализа угроз информационной безопасности в корпоративных системах

навыками маркетингового анализа ИКТ и вычислительного оборудования

методами анализа и оптимизации прикладных и информационных процессов

навыками работы с методами и типовыми средствами защиты информации в вычислительных системах и сетях

5. ФОРМЫ КОНТРОЛЯ И ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость: 144 / 4

Форма промежуточной аттестации: Экзамен

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование разделов и тем / вид занятия/

Раздел . Проблемы безопасности корпоративной информации. Технологии защиты корпоративных данных

Тема 1.1. Основные понятия и анализ угроз /Лек/

Тема 1.1. Основные понятия и анализ угроз /Пр/

Тема 1.1. Основные понятия и анализ угроз /Ср/

Тема 1.2. Политика информационной безопасности /Лек/

Тема 1.2. Политика информационной безопасности /Пр/

Тема 1.2. Политика информационной безопасности /Ср/

Тема 1.3. Криптографическая защита информации /Лек/

Тема 1.3. Криптографическая защита информации /Пр/

Тема 1.3. Криптографическая защита информации /Ср/

Тема 1.4. Идентификация, аутентификация и управление доступом /Лек/

Тема 1.4. Идентификация, аутентификация и управление доступом /Пр/

Тема 1.4. Идентификация, аутентификация и управление доступом /Ср/

Тема 1.5. Защита электронного документооборота /Лек/

Тема 1.5. Защита электронного документооборота /Пр/

Тема 1.5. Защита электронного документооборота /Ср/

Раздел . Комплексная защита корпоративных информационных систем

Тема 2.1. Принципы комплексной защиты информации КИС /Лек/

Тема 2.1. Принципы комплексной защиты информации КИС /Пр/

Тема 2.1. Принципы комплексной защиты информации КИС /Ср/

Тема 2.2 Защита от вредоносных программ /Лек/

Тема 2.2 Защита от вредоносных программ /Пр/

Тема 2.2 Защита от вредоносных программ /Ср/

Тема 2.3 Обнаружение и предотвращение вторжений /Лек/

Тема 2.3 Обнаружение и предотвращение вторжений /Пр/

Тема 2.3 Обнаружение и предотвращение вторжений /Ср/

Тема 2.4 Межсетевое экранирование /Лек/

Тема 2.4 Межсетевое экранирование /Пр/

Тема 2.4 Межсетевое экранирование /Ср/

Тема 2.5 Виртуальные защищенные сети VPN /Лек/

Тема 2.5 Виртуальные защищенные сети VPN /Пр/

Тема 2.5 Виртуальные защищенные сети VPN /Ср/

Раздел . Управление информационной безопасностью

Тема 3.1 Управление средствами обеспечения информационной безопасности /Лек/

Тема 3.1 Управление средствами обеспечения информационной безопасности /Пр/

Тема 3.1 Управление средствами обеспечения информационной безопасности /Ср/

Тема 3.2 Стандарты информационной безопасности /Лек/

Тема 3.2 Стандарты информационной безопасности /Пр/

Тема 3.2 Стандарты информационной безопасности /Ср/

Составитель(и): канд. экон. наук, доцент Тарусина Н.Э.