АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Информационная безопасность»

по основной профессиональной образовательной программе по направлению подготовки 38.03.05 «Бизнес-информатика» (уровень бакалавриата)

Направленность (профиль): Цифровая экономика
Общий объем дисциплины – 2 з.е. (72 часов)
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

- ОК-3: способностью использовать основы экономических знаний в различных сферах деятельности;
- ОПК-2: способностью находить организационно-управленческие решения и готов нести за них ответственность; готов к ответственному и целеустремленному решению поставленных профессиональных задач во взаимодействии с обществом, коллективом, партнерами;
- ПК-11: умение защищать права на интеллектуальную собственность;
- ПК-21: умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия;
- ПК-5: проведение обследования деятельности и ИТ-инфраструктуры предприятий;

Содержание дисциплины:
Дисциплина «Информационная безопасность» включает в себя следующие разделы:
Форма обучения заочная. Семестр 7.
1. Основные понятия и определения информационной безопасности.. Понятие и задачи информационной безопасности. надежность работы компьютера; сохранность ценных данных; защиту информации от внесения в нее изменений неуполномоченными лицами; сохранение тайны переписки в электронной связи..
2. Современные методы шифрования данных.. Обзор методов шифрования. Базовая математика шифровальных техник. Уязвимости и методы взлома и противодействия им.RSA. Протокол Диффи-Хеллмана. Математика, лежащая в основе двухключевых методов шифрования. Уязвимости и анализ атак..
3. Современные системы идентификации и аутентификации пользователей.. Существующие системы аутентификации пользователей. Парольные системы. Анализ взломостойкости и уязвимости..
Форма обучения очная. Семестр 6.
1. Основные понятия и определения информационной безопасности.. Понятие и задачи информационной безопасности. надежность работы компьютера; сохранность ценных данных; защиту информации от внесения в нее изменений неуполномоченными лицами; сохранение тайны переписки в электронной связи..
2. Современные системы идентификации и аутентификации пользователей.. Существующие системы аутентификации пользователей. Парольные системы. Анализ взломостойкости и уязвимости..
3. Биометрические системы аутентификации. Средства контроля доступа и аутентификации, использующие биометрию. Анализ уязвимостей..
4. Нормативно-правовые аспекты информационной безопасности.. Как защищать информацию законно. Анализ законодательной базы информационной безопасности..
5. Базовые методы шифрования.. Обзор методов шифрования. Базовая математика шифровальных техник. Уязвимости и методы взлома и противодействия им..
6. Технология инфраструктуры открытых ключей.. RSA. Протокол Диффи-Хеллмана. Математика, лежащая в основе двухключевых методов шифрования. Уязвимости и анализ атак..
7. Вредоносные программы.. Компьютерные вирусы. Методы получения контроля над зараженным компьютером. Методы противодействия..
8. Организация отдела информационной безопасности.. Применение методов информационной безопасности в реальной деятельности компании.

Разработал:
доцент
кафедры ИСЭ М.С. Жуковский
доцент
кафедры ИСЭ М.С. Жуковский
Проверил:
Декан ФИТ А.С. Авдеев