Аннотация
к рабочей программе дисциплины (модуля)«Компьютерные сети и информационная безопасность»
По направлению *38.03.01 Экономика*
(профиль *Экономика предприятий и организаций,* профиль *Бухгалтерский учет, анализ и аудит*)

Общая трудоемкость дисциплины составляет 6 зачетных единицы 216 часов.

Форма контроля: экзамен, курсовая работа, зачет

Предполагаемые семестры: 7,8-очное, 8,9-заочное

Цели:

Целями преподавания дисциплины являются:

- предоставление обучаемым знаний основных типов и способов защиты информации; приобретение студентами умения проектировать системы защиты информации; овладение современными программными и аппаратными средствами защиты информации.

Дисциплина «Компьютерные сети и информационная безопасность» относится к обязательным дисциплинам вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 38.03.01 «Экономика».

Для успешного освоения данной дисциплины необходимы базовые и специальные **знания,** полученные при изучении ОПОП бакалаврской подготовки, **знания**, полученные при изучении предшествующих дисциплин: «Информатика», «Информационные технологии в профессиональной деятельности» данной ОПОП; **умения** применять сетевые средства вычислительной техники для решения практических задач; **владения** навыками профессиональной работы в сетях ЭВМ с использованием современного программного обеспечения..

Краткое содержание дисциплины:

Раздел № 1. Общие вопросы информационной безопасности

Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.

Раздел № 2. Государственная система информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Раздел № 3. Угрозы безопасности

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Раздел № 4. Теоретические основы методов защиты информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Раздел № 5. Методы защиты средств вычислительной техники

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

Раздел № 6. Основы криптографии

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации.

Раздел № 7. Архитектура защищенных экономических систем

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.

Раздел № 8. Алгоритмы привязки программного обеспечения к аппаратному окружению
Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.
Раздел № 9. Алгоритмы безопасности в компьютерных сетях
Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

В результате освоения дисциплины бакалавр должен обладать следующими общекультурными и профессиональными компетенциями:

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);

способностью осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач (ОПК-2);

способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-8);

Заведующий Кафедрой САПР _____ И.Ю. Петрова