АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина Б1.В.ДВ.8 Защита информации

Семестр: 5
Количество часов: 108
Количество зачетных единиц: 3
Курсовая работа: -
Промежуточная аттестация: зачет

Место дисциплины в структуре ООП:

Дисциплина «Защита информации» относится к дисциплинам по выбору вариативной части базового блока Дисциплины (модули) Б1.В.ДВ.8 учебного плана подготовки бакалавра по направлению 09.03.03 *Прикладная информатика* направленность «Прикладная информатика в информационной сфере».

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин: «Правоведение», «Информационное общество и бизнес», «Проблемы и перспективы информационного общества», «Информационные системы и технологии», дополняет дисциплины: «Информационная безопасность», «Компьютерные справочно-правовые системы».

Освоение дисциплины «Защита информации» необходимо как предшествующее при изучении следующих дисциплин: «Операционные системы», «Программирование», «Организационное и правовое обеспечение информационной безопасности», «Мировые информационные ресурсы», «Метрология, стандартизация и сертификация», «Сети и телекоммуникации», «Сетевая экономика».

Цель дисциплины: понимание моделей и стандартов информационной безопасности, усвоение методов защиты информационных систем, приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.

Задачи:

- изучение и классификация причин нарушений безопасности;
- проектирование мониторов безопасности субъектов и объектов;
- приобретение практических навыков работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

Содержание дисциплины:

Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Безопасность в экономической сфере России.

Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. Соперничество в информационной сфере, информационные войны. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.

Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. Место, цели и задачи информационной безопасности в бизнесе. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации. Научные взгляды, теории и дискуссии. Концепция защиты информации. Понятие и цели защиты информации, формирование и эволюция понятия. Обеспечивающий технологический аспект защиты информации.

Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации. Понятие уязвимости информации. Типовые классификационные группы ценной предпринимательской информации. Информационные ресурсы государственные и негосударственные. Классификация информационных про-

дуктов и услуг. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.

Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции. Промышленный и экономический шпионаж, его сущность, история и сфера распространения. Легальные способы получения ценной и конфиденциальной информации, их состав. Нелегальные (противоправные, незаконные) способы получения ценной и конфиденциальной информации, их состав. Понятия злоумышленника, постороннего и случайного лица. Понятие и классификация источников конфиденциальной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. Интерес к информации как предпосылка возникновения угрозы. Понятие угрозы (опасности) информации, виды угроз. Риск угрозы и механизм реализации угрозы. Понятие несанкционированного канала утраты конфиденциальной информации. Случайные и преднамеренные условия возникновения этого канала. Поиск или формирование такого канала злоумышленником. Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. Характеристика каждого канала. Классификация технических каналов утечки конфиденциальной информации. Характеристика каждого канала. Комплексность использования организационных и технических каналов. Особенности структуры каналов распространения информации в компьютерах, локальных сетях, оргтехнике и средствах связи. Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений.

Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Промышленная собственность. Промышленные образцы. Информация о происхождения товара. Собственность на результаты творческого труда. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм патентного права. Характеристика норм авторского права и смежных прав. Торговый знак, знак обслуживания, торговая марка, фирменное наименование, эмблема предприятия. Страхование ценной информации. Законодатель-

ные акты, охраняющие вещную собственность на документированную информацию. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Организация деятельности средств массовой информации. Отношения средств массовой информации с гражданами и организациями. Ответственность за нарушение законодательства о средствах массовой информации.

Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Защита государственной тайны. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна. Тайны личная и семейная. Понятия - "фирменные секреты", "технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)". Документированная информация (документы) секретная и несекретная. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Сущность термина, особенности и условия применения, дискуссионность. Правовые и технологические аспекты присвоения информации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности. Деление документов на документы кратковременного и долговременного периода конфиденциальности. Конфиденциальность информации в вычислительных системах и сетях.

Понятие аналитической работы, ее цели и задачи. Аналитическая работа по выявлению каналов несанкционированного доступа к информации. Аналитическая работа с источником конфиденциальной информации. Аналитическая работа с источником угрозы конфиденциальной информации. Аналитическая работа с каналом объективного распространения информации. Стадии аналитической работы. Порядок и методика сбора исходных сведений, их анализа и оценки. Экспертные системы. Результаты аналитической работы как основа формирования системы защиты информации и ее совершенствования. Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принцип коллегиальности контроля. Принципы надежности и превентивности. Принцип эволюции структуры системы в условиях реальных угроз информации. Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской инфор-

мации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны. Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Цели и задачи перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Место перечня в системе защиты информации. Классификация ценной информации в предпринимательских структурах различного типа. Принципы определения состава ценных сведений, подлежащих защите в конкретной фирме. Перечни инвентарные и матричные. Структура перечней различных типов. Перечни списочные и проблемно-ориентированные. Организационные формы составления и ведения перечней. Содержание процедуры разработки перечня. Существующие методики сбора, анализа и обобщения сведений. Место маркетингового исследования в процедуре разработки перечня. Разграничение уровня конфиденциальности сведений, определение срока конфиденциальности, регламентация места документирования, использования и хранения, состава сотрудников, которым эти сведения необходимы для работы. Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация права предпринимательской структуры на защиту своей тайны. Регламентация структуры и содержания комплексной системы защиты информации фирмы. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.

Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и

функции аналитического подразделения. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций.

Физические средства защиты. Угрозы безопасности собственности фирмы и персоналу. Виды охраняемых объектов, категории защищаемых помещений. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны. Построение системы охраны объекта, многорубежная охрана. Классификация и характеристика классификационных групп технических средств охраны. Охранные системы. Охранное телевидение. Ограждение и физическая изоляция. Запирающие устройства. Методы взаимодействия охраны с техническими средствами сигнализации/оповещения, информирования, идентификации и ограничения. Порядок сдачи под охрану и снятия с охраны объектов и помещений. Назначение и задачи пропускного режима. Порядок доступа в помещения различных категорий персонала. Контрольно-пропускные пункты. Системы контроля доступа. Виды пропусков и идентификаторов, их учет, непериодическое обновление и порядок выдачи, изъятия. Технические средства идентификации. Правила охраны транспортных средств и транспортируемой продукции фирмы. Правила охраны персонала фирмы. Классификация экстремальных (чрезвычайных) ситуаций. Порядок действий персонала охраны в типовых ситуациях. Аппаратные средства защиты.

Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ.

Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи.

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности (*знать* основные нормативно-правовые документы; виды угроз ИС и методы обеспечения информационной безопасности; *уметь* ориентироваться в системе законодательства и нормативно-правовых актов, регламентирующих сферу профессиональной деятельности; выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; *владеть навыками* извлечения необходимой информации из оригинального текста);

ОПК-1: способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий (*знать* нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий; *уметь* использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий; *владеть навыками* работы с нормативно-правовыми документами, международными и отечественными стандартами в области информационных систем и технологий);

ОПК-4: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (*знать* информационно-коммуникационные технологии; методы поиска, анализа документов, способы обработки и передачи информации; принципы обработки данных с применением информационно-коммуникационных технологий; информационную и библиографическую культуру; основные требования к информационной безопасности информационных систем; *уметь* применять информационные технологии для решения профессиональных задач с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; *владеть навыками* работы с компьютером как средством управления информацией и решения стандартных задач профессиональной деятельности);

ПК-18: способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью *(знать* организацию и состав ИТ-инфраструктуры; *уметь* использовать программно-технические средства обеспечения информационной безопасности в организации ИТ-инфраструктуры и управлении информационной безопасностью; *иметь опыт* участия в организации ИТ-инфраструктуры и управлении информационной безопасностью).

Образовательные технологии:

Дисциплина «Защита информации» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий в зависимости от вида и цели учебного занятия: компьютерные симуляции, деловые и ролевые игры, мастер-классы, разбор конкретных ситуаций.

Теоретический материал излагается на лекционных занятиях в форме проблемно-ориентированных лекций.

Практические занятия ориентированы на закрепление теоретического материала, изложенного на лекционных занятиях, а также на приобретение дополнительных знаний, умений и практических навыков осуществления аналитической и профессиональной деятельности с применением интерактивных форм обучения (моделирования угроз информационной безопасности).

Составитель: К. С. Смолич, канд. техн. наук, доцент кафедры информатики и естественнонаучных дисциплин.