АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина Б1.В.ДВ.9 Организационное и правовое обеспечение информационной безопасности

Семестр: 6
Количество часов: 108
Количество зачетных единиц: 3
Курсовая работа: -
Промежуточная аттестация: зачет

Место дисциплины в структуре ООП:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам по выбору вариативной части блока «Дисциплины (модули)» Б1.В.ДВ.9 учебного плана подготовки бакалавра по направлению 09.03.03 *Прикладная информатика* направленность «Прикладная информатика в информационной сфере».

Дисциплина предполагает предварительное изучение обучающимися дисциплин: «Правоведение», «Информационное общество и бизнес», «Проблемы и перспективы информационного общества», «Информационная безопасность», «Защита информации», «Компьютерные справочно-правовые системы», имеет преемственную связь с дисциплинами: «Операционные системы», «Программирование», «Мировые информационные ресурсы».

Изучение дисциплины «Организационное и правовое обеспечение информационной безопасности» является основой для дальнейшего изучения дисциплин: «Метрология, стандартизация и сертификация», «Сети и телекоммуникации».

Цель дисциплины: формирование у обучающихся систематизированных знаний об организации мероприятий по информационной безопасности на объекте информатизации и их правовом обеспечении.

Задачи:

− изучить основы законодательства Российской Федерации, касающиеся системы защиты государственной и коммерческой тайны, правил лицензирования и сертификации в области защиты информации;

− изучить методы организационного обеспечения информационной безопасности на объекте информатизации;

− сформировать навыки составления плановых документов и корпоративных нормативно-правовых актов, обеспечивающих информационную безопасность на объекте информатизации.

Содержание дисциплины:

Понятие информационной безопасности в широком и узком смысле. Объекты информационной безопасности на уровне государства, общества и

предприятия и их угрозы. Национальные интересы в информационной сфере РФ. Принципы деятельности по осуществлению информационной безопасности РФ и формы осуществления этой деятельности. Правовые нормы, обеспечивающие информационную безопасность на уровне личности, государства и предприятия. Основные нормативно-правовые акты, регулирующие защиту конфиденциальной информации: ФЗ «О коммерческой тайне», «О государственной тайне», «О связи», «Об информации, информационных технологиях и о защите информации», «Об электронной подписи» и др. Виды тайн, защищаемых законодательством РФ.

ФЗ «О коммерческой тайне»: понятие коммерческой тайны и режима коммерческой тайны; порядок установления режима коммерческой тайны; обязанности работника, работодателя и контрагентов по защите установленного режима; дисциплинарная, гражданско-правовая, административная и уголовная ответственность за нарушение этого закона. ФЗ «О государственной тайне»: основные понятия закона; принципы отнесения информации к государственной тайне; грифы секретности; основания для рассекречивания сведений, составляющих государственную тайну; порядок допуска должностных лиц, граждан, предприятий к сведениям, составляющим государственную тайну; ответственность за нарушение этого закона. Лицензирование деятельности по защите информации и сертификация средств защиты: нормативно-правовые акты и современная практика. Объекты авторских и смежных прав. Патентное право. Право на топологии интегральных микросхем. Право на секрет производства. Право на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий.

Понятие угрозы и ее свойства. Классификация угроз. Источники конфиденциальной информации на предприятии. Каналы утечки информации и их виды. Оценка ущерба предприятия вследствие разглашения конфиденциальной информации. Основные направления защиты конфиденциальной информации на предприятии. Принципы организационной защиты информации. Основные подходы и требования к организации системы защиты информации. Структура управления системой защиты информации. Методы, средства и привлекаемые подразделения для организации защиты информации на предприятии.

Состав и характеристика массива нормативных документов по защите информации на предприятии. Политика безопасности: структура и требования к составлению. Назначение Концепции информационной безопасности. Этапы внедрения политики информационной безопасности на предприятии.

Разрешительная система доступа персонала к конфиденциальной информации. Порядок доступа к конфиденциальной информации командированных лиц. Порядок приема посетителей на предприятии. Организационные и психологические причины разглашения персоналом конфиденциальной информации. Основные этапы работы с персоналом на предприятии: прием кандидата на работу, в ходе исполнения должностных обязанностей, перевод на другую должность, в процессе увольнения. Методы работы с сотрудниками. Мотивация деятельности персонала: факторы, влияющие на успешность;

методы стимулирования сознательности персонала в области защиты информации.

Организация пропускного режима: принципы организации и привлекаемые структурные подразделения. Виды пропусков. Организация охраны и физической защиты объектов предприятия: объекты защиты, цели и принципы. Состав службы охраны. Права и обязанности сотрудников охраны. Технические средства, применяемые для организации охраны и физической защиты.

Цели планирования. Структура типовых планов по защите информации в повседневной деятельности, при проведении совещаний, в ходе публикаторской и рекламной деятельности, при работе со СМИ. Виды аккредитации журналистов при предприятии. Формы работы со СМИ. Контроль: цели, задачи, объекты, формы проведения. Применяемые методы контроля: проверка, учет, сравнение, наблюдение, анализ. Виды проверок. Алгоритм подготовки и проведения проверки. Анализ состояния защиты информации: объекты, функции аналитического подразделения. Меры, принимаемые по результатам аналитической работы. Этапы аналитической работы. Методы анализа информации. Аналитический отчет: виды и типовая структура.

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; информаци-

онную 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).

Образовательные технологии:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» 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 (моделирование деловых ситуаций, подготовка презентаций, групповые дискуссии).

С целью формирования и развития профессиональных навыков студентов предлагается использовать проектную технологию, портфолио, визуальные презентации теоретического материала.

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