

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Б.3.ДВ.01 Организационное и правовое обеспечение информационной безопасности

Семестр: 5

Количество часов: 108

Количество зачетных единиц: 3

Промежуточная аттестация: зачет

Место дисциплины в структуре ООП:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплине по выбору профессионального цикла Б.3.ДВ.01 учебного плана направления 09.03.03 (230700.62) *Прикладная информатика* профиль «Прикладная информатика в информационной сфере».

Данная дисциплина содержательно дополняет дисциплину «Информационная безопасность».

Цель и задачи освоения дисциплины:

Цель дисциплины «Организационное и правовое обеспечение информационной безопасности» дать студентам систематизированные знания об организации мероприятий по информационной безопасности на объекте информатизации и об их правовом обеспечении.

Для достижения поставленной цели студентам необходимо решить следующие основные 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, ин-

формационных 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 охра-

ны 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 учебной дисциплины обучающийся должен обладать следующими общекультурными (ОК) и профессиональными (ПК) компетенциями:

ОК-7 способен понимать сущность и проблемы развития современного информационного общества (*знать* отличительные особенности электронного бизнеса и электронной коммерции, типологию современной сетевой экономики, методы маркетинговых исследований в Интернете; *уметь* планировать, проектировать и оценивать использование среды Интернет во всех сферах предпринимательской деятельности; *владеть* методами управления процессами, связанными с Интернетом, учитывая самые современные технологии).

ОК-8 способен работать с информацией в глобальных компьютерных сетях (*знать* возможности глобальных компьютерных сетей; *уметь* осуществлять поиск информации в глобальных компьютерных сетях; *владеть* веб-технологиями).

ОК-12 способен использовать Гражданский кодекс Российской Федерации, правовые и моральные нормы в социальном взаимодействии и реализации гражданской ответственности (*знать* методы и средства для укрепления здоровья; *уметь* использовать их в своей профессиональной деятельности; *владеть* современными методиками здорового образа жизни).

ОК-13 способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государства (*знать* основные проблемы, возникающие при информатизации социально-экономических задач; *уметь* использовать программно-технические средства обеспечения информационной безопасности; *владеть* навыками организации мероприятий по обеспечению информационной безопасности).

ПК-1 способен использовать нормативные правовые документы в профессиональной деятельности (*знать* основные нормативные правовые документы, регламентирующие деятельность в профессиональном поле; *уметь* сле-

доть за изменениями нормативных правовых документов, регламентирующих деятельность в профессиональном поле; уметь использовать нормативные правовые документы в своей деятельности; *владеть* навыками анализа нормативных и правовых документов, использовать их в профессиональной деятельности).

ПК-4 способен ставить и решать прикладные задачи с использованием современных информационно-коммуникационных технологий (*знать* типовые модели решения задач; *уметь* ставить задачу исходя из проблемной ситуации и решать ее с помощью типовых моделей и современных информационно-коммуникационных технологий; *владеть* разнообразными современными информационно-коммуникационными технологиями).

ПК-18 способен анализировать и выбирать методы и средства обеспечения информационной безопасности (*знать* основные понятия и концепцию информационной безопасности; основные средства и способы защиты информации; *уметь* выявлять и классифицировать основные угрозы безопасности информации; *владеть* средствами средства защиты информации от разглашения, разрушения, несанкционированного доступа и т.д.).

ПК-19 способен анализировать рынок программно-технических средств, информационных продуктов и услуг для решения прикладных задач и создания информационных систем (*знать* особенности информационных продуктов и услуг для решения прикладных задач; принципы формирования цен на продукцию высоких технологий и других сетевых товаров; *уметь* использовать принципы и законы сетевой экономики в традиционных отраслях сбыта услуг и продукции; *владеть* методиками анализа рынка программно-технических средств, информационных продуктов и услуг).

ПК-20 способен выбирать необходимых для организации информационные ресурсы и источники знаний в электронной среде (*знать* организацию информационных и финансовых служб фирм на основе современных компьютерных, информационных технологий; электронные службы и электронные платежные системы; *уметь* использовать полученные знания при организации работы офиса, бухгалтерии, отделов сбыта и других управленческих подразделений организации; *владеть* навыками работы в платежных системах, электронных службах, на виртуальных биржах и аукционах; методами поиска информации в сети Интернет).

ПК-22 способен готовить обзоры научной литературы и электронных информационно-образовательных ресурсов для профессиональной деятельности (*знать* источники информационно-образовательных ресурсов; *уметь* готовить обзоры научной литературы и электронных информационно-образовательных ресурсов; *владеть* информационно-образовательными технологиями).

Образовательные технологии:

Дисциплина 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.

Лабораторные 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, к. т. н, доцент кафедры прикладной информатики