

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ «Организационное и правовое обеспечение информационной безопасности»

по основной профессиональной образовательной программе по направлению подготовки
10.03.01 «Информационная безопасность» (уровень бакалавриата)

Направленность (профиль): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)

Общий объем дисциплины – 6 з.е. (216 часов)

В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:

- УК-2.1: Анализирует поставленную цель и формулирует задачи, которые необходимо решить для её достижения;
- УК-2.2: Выбирает оптимальный способ решения задач с учётом существующих ресурсов и ограничений;
- УК-2.3: Выбирает правовые и нормативно-технические документы, применяемые для решения поставленных задач;
- ОПК-5.1: Осуществляет поиск необходимых нормативных правовых актов и нормативных методических документов;
- ОПК-5.2: Демонстрирует знание состава нормативной документации;
- ОПК-5.3: Использует нормативные правовые акты, нормативные методические документы в профессиональной деятельности;
- ОПК-6.1: Выбирает нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

Содержание дисциплины:

Дисциплина «Организационное и правовое обеспечение информационной безопасности» включает в себя следующие разделы:

Форма обучения очная. Семестр 3.

Объем дисциплины в семестре – 2 з.е. (72 часов)

Форма промежуточной аттестации – Зачет

1. Правовые основы в области ИБ. Информационная сфера и информация в системе права. Основные понятия права. Информационная сфера как предмет правового регулирования. Информация как объект права и защиты. Системы обработки, хранения и передачи информации как объекты права. Содержание и структура правового обеспечения информационной безопасности. Роль права в регулировании комплекса отношений в области информационной безопасности. Понятие, предмет и содержание правового обеспечения информационной безопасности. Принципы правового регулирования отношений, связанных с обеспечением информационной безопасности.

Структура законодательства в области информационной безопасности, состав нормативной документации. Основные законодательные акты по видам защиты информации. Использование нормативных правовых актов, нормативных методических документов в профессиональной деятельности. Правовые основы защиты информации. Принципы правового регулирования отношений по защите информации. Цели и задачи защиты информации. Правовая защита информации ограниченного доступа. Правовой режим защиты информации. Ответственность за правонарушения в области защиты информации. Правовые основы деятельности и функции органов, обеспечивающих информационную безопасность. Органы, обеспечивающие информационную безопасность в Российской Федерации. Межведомственные комиссии. Федеральная служба безопасности России. Федеральная служба по техническому и экспортному контролю..

2. Правовые режимы. Лицензирование и сертификации в области защиты информации. Основные понятия и источники права по лицензированию в области защиты информации. Лицензируемые виды деятельности. Сертификация средств защиты информации.

Государственная тайна как объект права. Отнесение сведений к государственной тайне, их

засекречивание и рассекречивание. Распоряжение информацией, составляющей государственную тайну. Режим и органы защиты государственной тайны. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну. Правовая основа допуска должностных лиц и граждан к государственной тайне. Контроль и надзор за обеспечением защиты государственной тайны.

Коммерческая тайна как объект права. Отнесение информации к ИСКТ. Охрана конфиденциальности информации. Режим коммерческой тайны. Субъекты права на коммерческую тайну и их обязанности по охране конфиденциальности ИСКТ. Нормативное правовое обеспечение режима коммерческой тайны организации.

Персональные данные как особый институт охраны права на неприкосновенность частной жизни. Персональные данные как объект права и защиты. Субъекты правоотношений связанных с обработкой персональных данных их права и обязанности. Обеспечение безопасности персональных данных при их обработке. Правовые основы обеспечения безопасности критической информационной инфраструктуры. Полномочия органов власти в области обеспечения безопасности КИИ. Категорирование объектов КИИ. Права и обязанности субъектов КИИ..

3. Правовые вопросы в сфере информационной безопасности. Понятие интеллектуальной деятельности и интеллектуального продукта. Институты права и объекты интеллектуальной собственности. Интеллектуальные права. Распоряжение исключительным правом. Защита интеллектуальных прав.

Преступления в сфере компьютерной информации. Классификация компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание и распространение вредоносных программ для ЭВМ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Правовая ответственность за нарушения законодательства о государственной тайне. Виды правовой ответственности за нарушения законодательства о государственной тайне. Виды посягательств на государственную тайну. Уголовная ответственность за посягательства на государственную тайну. Административная и дисциплинарная ответственность за нарушения в области защиты государственной тайны. Правовая ответственность за нарушения законодательства о тайнах и об интеллектуальной собственности. Ответственность за нарушение законодательства о коммерческой тайне. Ответственность за нарушение законодательства о персональных данных. Ответственность за нарушение законодательства о служебной и профессиональной тайне. Ответственность за нарушение законодательства об интеллектуальной собственности..

Форма обучения очная. Семестр 4.

Объем дисциплины в семестре – 4 з.е. (144 часов)

Форма промежуточной аттестации – Экзамен

1. Сущность организационного обеспечения информационной безопасности. Сущность организационного обеспечения информационной безопасности. Организация работы по определению состава, засекречиванию и рассекречиванию информации. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Организация системы доступа к защищаемой информации (сведениям, документам, изделиям)..

2. Организационная деятельность на предприятии. Анализ поставленной цели защиты информации и формулировка задач, которые необходимо решить для её достижения. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации. Организация охраны предприятия и физической защиты его объектов. Организация пропускного и внутриобъектового режимов. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями. Выбор правовых и нормативно-технических документов, применяемых для решения поставленных задач, в том числе нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

3. Организация защиты информации. Выбор оптимальных способов решения задач защиты информации с учётом существующих ресурсов и ограничений. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности. Защита

информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу. Организация служебного расследования по фактам разглашения конфиденциальной информации или утраты носителей информации..

Разработал:
доцент
кафедры ИВТиИБ

А.В. Санников

Проверил:
Декан ФИТ

А.С. Авдеев