

АННОТАЦИЯ

рабочей программы дисциплины «Организационное и правовое обеспечение информационной безопасности»

по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата)

Направленность (профиль) образовательной программы:

Прикладная информатика в юриспруденции

Цель освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» – формирование у обучающихся целостной системы знаний в области правового регулирования и организационного обеспечения информационной безопасности, развитие навыков применения нормативно-правовых актов при проектировании, внедрении и эксплуатации систем защиты информации, а также формирование компетенций по управлению рисками информационной безопасности в соответствии с требованиями законодательства Российской Федерации.

Место дисциплины в структуре образовательной программы бакалавриата

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к части формируемой участниками образовательных отношений.

Освоение дисциплины предполагает наличие у обучающихся знаний, умений и навыков по дисциплинам: «Теория государства и права», «Информационные технологии», «Технологии и методы программирования», «Правоохранительные органы Российской Федерации».

Знания, полученные в результате освоения дисциплины, являются базовыми для прохождения учебной и производственной практик, а также для выполнения выпускной квалификационной работы по направлению подготовки.

Объем, структура и содержание дисциплины «Организационное и правовое обеспечение информационной безопасности» составляет 3 зачетных единицы, 108 академических часов.

Содержание дисциплины «Организационное и правовое обеспечение информационной безопасности»

Раздел 1. Правовые основы информационной безопасности в Российской Федерации

Тема 1. Конституционные основы и федеральное законодательство в сфере информационной безопасности.

Конституционные гарантии права на информацию и защиту частной жизни. Федеральный закон «О безопасности»: основные положения, полномочия органов государственной власти в сфере ИБ. Федеральный закон «Об информации, информационных технологиях и о защите информации»: классификация информации, порядок ограничения доступа к информации, ответственность за нарушение требований законодательства. Федеральный закон «О защите информации, содержащейся в информационных системах персональных данных» (в ред. ФЗ от 27.07.2006 № 152-ФЗ). Классификация информации по степени секретности: государственная тайна, служебная тайна, коммерческая тайна. Правовые основы лицензирования деятельности в области защиты информации. Международно-правовые аспекты обеспечения информационной безопасности.

Тема 2. Правовое регулирование защиты персональных данных и коммерческой тайны.

Федеральный закон «О персональных данных»: основные понятия, принципы и условия обработки персональных данных, права субъектов персональных данных, обязанности операторов. Требования к защите персональных данных при их обработке в информационных системах. Порядок уведомления об обработке персональных данных.

Ответственность за нарушение законодательства о персональных данных. Правовое регулирование коммерческой тайны: понятие, условия отнесения информации к коммерческой тайне, меры по обеспечению конфиденциальности. Судебная практика по делам о нарушении законодательства в сфере защиты персональных данных и коммерческой тайны.

Раздел 2. Организационное обеспечение информационной безопасности

Тема 3. Система управления информационной безопасностью: стандарты, политики, регламенты.

Международные стандарты в области ИБ: серия стандартов ISO/IEC 27000. Государственные стандарты РФ: ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Структура и содержание политики информационной безопасности организации. Разработка локальных нормативных актов по ИБ: регламенты доступа к информации, инструкции по обработке персональных данных, положения о коммерческой тайне. Организационная структура обеспечения ИБ в организации: распределение ответственности, формирование рабочих групп. Требования нормативных актов к документальному оформлению системы управления ИБ.

Тема 4. Оценка рисков и разработка организационных мер защиты информации.

Методология оценки рисков информационной безопасности: идентификация активов, угроз и уязвимостей, анализ последствий реализации угроз. Риск-ориентированный подход к управлению ИБ. Разработка организационных мер защиты информации: регламентация доступа к информации, обучение персонала, контроль соблюдения политик ИБ. Планирование мероприятий по снижению рисков ИБ с учетом экономической целесообразности и правовых ограничений. Организация аудита системы управления ИБ: внутренний и внешний аудит, сертификация по стандартам. Документирование результатов оценки рисков и планов по их снижению.