АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Правовое обеспечение информационной безопасности

Автор: Мерзляков С. Э.

Код и наименование направления подготовки, профиля:

40.05.01 Правовое обеспечение национальной безопасности, специализация: уголовно-правовая

Квалификация (степень) выпускника: юрист

Форма обучения: очная

Цель освоения дисциплины:

Формирование способности внедрять новые технологии и методики противодействия угрозам национальной безопасности. Формирование умения анализировать состояние текущей деятельности организации (органа, места работы) с позиций ее безопасности; проводить исследования текущей практической деятельности органов и организаций, отдельных направлений этой деятельности в целях выявления уязвимости действующих систем безопасности и своевременного принятия мер по их усилению, модернизации и повышению уровня безопасности; применять методики предотвращения инцидентов безопасности, правонарушений, реагирования на правонарушения и инциденты безопасности в текущей деятельности органов и организаций

Содержание дисциплины:

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Понятие ИБ и информационного общества.

Цели, задачи и принципы обеспечения ИБ.

Угроза национальной безопасности и их виды.

Информационные войны и информационное оружие. Информационный терроризм.

Информационное общество в РФ и его характеристики. Информационная сфера и ее области.

Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

Понятие правового обеспечения и правовой защиты.

История формирования законодательства РФ об информации и ее защите.

Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ.

Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ.

Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения.

Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ.

Правовое регулирование деятельности средств массовой информации.

Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

Информация, ее виды и признаки.

Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды.

Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны.

Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты.

Основные принципы засекречивания информации.

Конфиденциальная информация и возможные каналы ее утечки.

Информационная инфраструктура и информационная среда. Их структура и характеристики.

Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития.

Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Понятие государственного управления в сфере обеспечения ИБ.

Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности.

Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.

Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.

Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Понятие и виды преступности в информационной сфере.

Основные этапы и тенденции развития компьютерной преступности в России.

Особенности детерминации преступлений, совершаемых в информационной сфере.

Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет.

Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации.

Уголовно-правовая характеристика преступлений в сфере компьютерной информации.

Особенности объективных признаков компьютерных преступлений. Основные способы их совершения.

Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения.

Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.

Конституционные гарантии правовой охраны прав личности в информационной сфере.

Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.

Правовой механизм защиты права на неприкосновенность частной жизни.

Врачебная тайна как институт защиты интересов личности.

Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных.

Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

Понятие государственной тайны и правового режима ее обеспечения.

Принципы и механизм отнесения сведений к государственной тайне (ГТ).

Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну.

Субъекты обеспечения режима государственной тайны и их правовой статус.

Организационно-правовые меры защиты ГТ.

Допуск и доступ к ГТ.

Обеспечение ИБ при международном обмене информацией.

Система контроля за режимом обеспечения ГТ.

Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям.

Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.

Компьютерные преступления и особенности их идентификации и предупреждения.

Правовые основы применения «электронной цифровой подписи» (ЭЦП).

Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира.

Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа.

Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах.

Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС.

Правовой механизм обеспечения защиты авторских и смежных прав.

Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных.

Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства.

Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей.

Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак.

Программы для ЭВМ и механизм их правовой защиты.

Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

Понятие КТ и ее правовой статус.

Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель.

Объекты защиты КТ. Особенности правового обеспечения режима КТ.

Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ.

Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти.

Юридическая ответственность за нарушения режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ.

Понятие лицензирования по российскому законодательству.

Виды деятельности, подлежащие лицензированию в сфере ИБ.

Система государственного лицензирования в сфере ИБ и ее функции.

Субъекты лицензирования в сфере ИБ и их правовой статус.

Порядок лицензирования, приостановления или аннулирования действия лицензии.

Специальная экспертиза предприятия и государственная аттестация их руководителей.

Контроль за условиями обеспечения ИБ лицензиатами.

Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ.

Цели создания системы ССЗИ.

Организационная структура системы ССЗИ и особенности правового статуса ее субъектов.

Объекты сертификационной деятельности и режимы сертификации.

Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации.

Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Информационная безопасность России и задачи по ее обеспечению.

Система детерминант преступности в информационной сфере. Уровневый подход.

Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ.

Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус.

Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ.

Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ.

Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ.

Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны.

Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России.

Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ.

Составы административных правонарушений, посягающих на ИБ страны.

Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

Формы текущего контроля и промежуточной аттестации:

В ходе реализации дисциплины «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

При проведении занятий лекционного типа: опрос.

При проведении практических занятий: доклад, презентация, тесты.

Формой промежуточной аттестации выступает: экзамен

Этап(ы) освоения компетенции:

ОПК ОС-4.1.6: способность различными способами и с применением конкретной методики проводить мероприятия по снижению уровня опасности в деятельности органов и организаций

Результат формирования компетенции

на уровне знаний:

- о различных видах безопасности и правовом регулировании деятельности по безопасности;

- о видах угроз безопасности, о последствиях реализации этих угроз, о способах и методике проведения мероприятий по снижению уровня опасности в деятельности органов и организаций.

- Воспроизводит основные понятия, определения и категории информационной безопасности, умеет их раскрыть, прокомментировать.

Знает иерархию законодательного регулирования различных видов безопасности, называет законы и другие нормативные акты, умеет объяснить их содержание.

Ориентируется в политических, экономических, социальных процессах деятельности организации, используя правовые знания, основанные на этических постулатах.

Оценивает ситуации и события в деятельности организации с позиций ее безопасности.

Распознает проблемы, возникающие в практической деятельности, сопряженные с угрозами информационной безопасности организации.

Этап(ы) освоения компетенции:

ОПК ОС-5.1.7: способность выделять перспективные направления в национальной безопасности и реализации проектов внедрения новаций, учитывая развитие различных информационно-коммуникационных технологий

Результат формирования компетенции

на уровне знаний:

- о различных видах безопасности и правовом регулировании деятельности по безопасности;

- о видах угроз безопасности;

- о последствиях реализации этих угроз;

- о реализации органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

- о передовом отечественном и зарубежном опыте решения проблем безопасности;

о научных разработках в этой сфере.

Этап(ы) освоения компетенции:

ПСК-1.1.2.: способность применять в профессиональной деятельности законодательство, регулирующее общественные отношения в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере, а также использовать современные информационно-коммуникационные и высокие технологии в противодействии транснациональной организованной преступности

Результат формирования компетенции

на уровне знаний:

- об основных положениях, их назначении и политико-правовой основе стратегии развития информационного общества в Российской Федерации;
- о федеральных законах, а также нормативных правовых актах, определяющих направления социально-экономического развития, повышения эффективности государственного управления и взаимодействия органов государственной власти и гражданского общества в Российской Федерации;
- о новых формах правонарушений в сфере национальной безопасности и видах ответственности за них.

на уровне умений:

- применять в обеспечении информационной и национальной безопасности современные информационные, телекоммуникационные и иные высокие технологии;
- отстаивать свою принципиальную, основанную на нормах права, развитом правовом сознании, правовом мышлении и правовой культуре, профессиональную позицию;

на уровне навыков:

- навык обнаружения реальных и скрытых угроз информационной безопасности деятельности граждан, органов/организаций;
- опыт сбора значимой для принятия правового решения информации в сфере обеспечения национальной безопасности;

Основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.

2. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.