

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петренко Вячеслав Иванович
Должность: и.о. директора Института цифрового развития
Дата подписания: 05.07.2024 09:35:26
Уникальный программный ключ:
b47f96eea65a2dc27b94abf7bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Организационное и правовое обеспечение защиты информации
Содержание	Правовые основы информационной безопасности Российской Федерации. Предмет информационного права в информационной безопасности. Место информационного права в системе законодательства Российской Федерации. Структура правоотношений и виды юридической ответственности. Структура и состав информационного законодательства. Информация как объект права. Общая характеристика законодательства Российской Федерации в области информационной безопасности. Общие сведения о законодательстве Российской Федерации в области защиты информации. Федеральный закон «Об информации, информационных технологиях и о защите информации». Доктрина информационной безопасности Российской Федерации. Федеральный закон «О техническом регулировании». Закон Российской Федерации «О безопасности». Правовое регулирование отдельных видов информации. Правовое обеспечение защиты государственной тайны. Информация ограниченного доступа в сфере государственного и муниципального управления. Система документов по защите государственной тайны. Федеральный закон «О государственной тайне». Правовой режим защиты государственной тайны. Система защиты государственной тайны. Структура органов по защите государственной тайны Российской Федерации. Полномочия органов государственной власти и должностных лиц в области защиты государственной тайны. Допуск должностных лиц и граждан к государственной тайне. Контроль и надзор за обеспечением защиты государственной тайны. Правовое обеспечение защиты банковской, профессиональной и служебной тайны. Пользование информацией, составляющей банковскую тайну. Пользование информацией, составляющей профессиональную тайну. Пользование информацией, составляющей служебную тайну. Правовое обеспечение защиты коммерческой тайны. Перечень сведений конфиденциального характера. Законодательство Российской Федерации о коммерческой тайне. Федеральный закон «О коммерческой тайне». Информация, относящаяся к коммерческой тайне. Правовое обеспечение защиты персональных данных. Законодательство Российской Федерации о персональных данных. Ответственность за нарушение норм защиты персональных данных. Правовое обеспечение защиты интеллектуальной собственности. Понятие и структура интеллектуальной собственности. Объекты интеллектуальной собственности. Правовая охрана интеллектуальной собственности. Правовая охрана и защита патентного и авторского права. Общие положения патентного права. Правовая охрана и защита патентных прав. Общие положения об авторских и смежных правах. Правовая охрана и защита авторских и смежных прав. Система органов обеспечения информационной безопасности.

	Структура органов. Общие функции органов государственной власти в области информационной безопасности. Структура федеральных органов исполнительной власти. Общие сведения о Министерстве связи и массовых коммуникаций Российской Федерации. Общие сведения о Министерстве образования и науки Российской Федерации. Общие сведения о Министерстве внутренних дел Российской Федерации. Министерство связи и массовых коммуникаций Российской Федерации. Федеральное агентство по печати и массовым коммуникациям. Общие сведения о Федеральном агентстве по печати и массовым коммуникациям. Полномочия Федерального агентства по печати и массовым коммуникациям. Организация деятельности Федерального агентства по печати и массовым коммуникациям. Правовое регулирование деятельности по защите информации. Документы Гостехкомиссии России. Единые критерии, стандарты. Общая характеристика «Руководящих документов Гостехкомиссии России». Общие сведения об «Единых критериях безопасности информационных технологий» и ГОСТ Р ИСОМЭК 15408. Характеристика основных положений «Единых критериев». Анализ требований безопасности компонентов автоматизированных систем в рамках «Единых критериев». Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию ФСБ и ФСТЭК. Общие принципы лицензирования деятельности в области защиты информации. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСБ России. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСТЭК России. Порядок сертификации средств защиты информации. Общие сведения о сертификации средств защиты информации. Положение о сертификации средств защиты информации. Порядок проведения сертификации средств защиты информации по требованиям безопасности информации. Аттестация объектов информатизации в области защиты информации. Положение по аттестации объектов информатизации по требованиям безопасности информации. Требования к нормативным и методическим документам по аттестации объектов информатизации. Борьба с компьютерными преступлениями. Классификация компьютерных преступлений. Административная ответственность за правонарушения в сфере информации. Уголовная ответственность за правонарушения в сфере информации. Выявление компьютерных преступлений. Методики проведения следственных действий по расследованию компьютерных преступлений.
Реализуемые компетенции	ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации,

	Федеральной службы по техническому и экспортному контролю. ПК-1. Способен разрабатывать требования по защите информации для формирования политик безопасности компьютерных систем и сетей. ПК-2. Способен проводить анализ безопасности компьютерных систем. ПК-3. Способен проводить сертификацию программно-аппаратных средств защиты информации и анализ результатов. ПК-4. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения ПК-10. Способен проводить аттестацию объектов вычислительной техники на соответствие требованиям по защите информации
Результаты освоения дисциплины (модуля)	ОПК-5 Знать: источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации. Уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям

безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации.

Владеть: методами и средствами технической защиты информации.

ОПК-6

Знать: систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем;

Уметь: разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

ПК-1

Знать: принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации

Уметь: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты

информации.

Владеть: навыками разработки технических заданий на создание средств защиты информации; классификации информационной системы по требованиям защиты информации.

ПК-2

Знать: уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации.

Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей.

Владеть: навыками определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; подготовки аналитического отчета по результатам проведенного анализа; формулирования предложений по устранению выявленных уязвимостей.

ПК-3

Знать: национальные, межгосударственные и международные стандарты в области защиты информации; национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; принципы построения средств криптографической защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации.

Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; использовать профили защиты и задания по безопасности; применять инструментальные средства проведения сертификационных испытаний; составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям; делать выводы по

оценке защищенности на основании аналитического отчета.

Владеть: навыками проведения теоретических исследований уровней защищенности компьютерных систем и сетей; проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; проведения сертификационных испытаний с использованием инструментальных средств; подготовки аналитического отчета по результатам проведенных сертификационных испытаний; формулирования выводов по оценке защищенности.

ПК-4

Знать: принципы построения компьютерных систем и сетей; формальные модели безопасности компьютерных систем и сетей; принципы построения систем обнаружения компьютерных атак; методы обработки данных мониторинга безопасности компьютерных систем и сетей; порядок создания и структура отчета, создаваемого по результатам проверок; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; криптографические протоколы, применяемые в компьютерных сетях; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации.

Уметь: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.

Владеть: навыками выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнения анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составления отчетов по результатам проверок.

ПК-10

Знать: нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах; способы реализации несанкционированного доступа к информации и специальных программных воздействий на

	информацию и ее носители в компьютерных системах; способы защиты информации от утечки по техническим каналам; технические средства защиты информатизации от утечки за счет побочных электромагнитных излучений и наводок; методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее; программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа; порядок аттестации объектов информатизации на соответствие требованиям по защите информации; отчетные документы, оформляемые по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации. Уметь: разрабатывать программы и методики аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; проводить аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); оформлять аттестат соответствия объектов вычислительной техники требованиям по защите информации Владеть: навыками разработки программы и методик аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; подготовки заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации.
Трудоемкость, з.е.	7
Форма отчетности	Зачет, 8 семестр; экзамен, 9 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности Электронный ресурс: Учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. – Организационно-правовое и методическое обеспечение информационной безопасности, 2022-10-01. – Санкт-Петербург: Университет ИТМО, 2016. – 169 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 2227-8397, экземпляров неограничено 2. Организационное и правовое обеспечение информационной безопасности / А. Ф. Чипига, М. А. Лапина. – Ставрополь: СевКавГТУ, 2014. – 525 с.
Дополнительная	1. Правовое обеспечение информационной безопасности: учебник

литература	/ [под общ. науч. ред. В. А. Минаева и др.]. – Изд. 2-е, расш. и доп. – Москва: Маросейка, 2013. – 368 с.: ил., табл. – (Информатика и информационная безопасность). – Библиогр.: с. 360-368. 2. Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / под ред. С. Я. Казанцева. – 3-е изд., стер. – М.: Академия, 2015. – 240 с.: ил., рис., табл. – (Высшее профессиональное образование). – Прил.: с. 224-22 3. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью». Выпуск 1 Милославская Н.Г. Сенаторов М.Ю. Толстой А.И. Издательство: "Горячая линия-Телеком" ISBN: 978-5-9912-0271-8; 2011: 244 с. 4. Голиков А.М. Основы информационной безопасности Издательство: ТУСУР (Томский государственный университет систем управления и радиоэлектроники) ISBN: 978-5-868889-467-1 2018, 201 с. 5. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности Электронный ресурс: Учебное пособие / Г. П. Жигулин. – Организационное и правовое обеспечение информационной безопасности, 2022-10-01. – Санкт-Петербург: Университет ИТМО, 2014. – 174 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 2227-8397, экземпляров неограниченно
------------	---