

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:
 b47f96eeab5410e175f94ab1fb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Основы информационной безопасности
Содержание	Основные сведения о национальной и информационной безопасности РФ. Терминологические основы информационной безопасности. Общеметодологические принципы теории информационной безопасности. Источники возникновения угроз информационной безопасности. Способы реализации угроз информационной безопасности и результаты их воздействия. Методы нарушения конфиденциальности, целостности и доступности информации. Каналы утечки и искажения информации. Анализ моделей действия «нарушителя». Методы оценки уязвимости и защищенности информации. Основные направления обеспечения информационной безопасности объектов. Стратегии и системы обеспечения информационной безопасности. Модели и методы обеспечения информационной безопасности компьютерных систем.
Реализуемые компетенции	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства. ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
Результаты освоения дисциплины (модуля)	ОПК-1 Знать: понятия информации, информационных технологий, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; Уметь: применять современные информационные технологии в профессиональной деятельности, классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: способностью оценивания роли информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства. 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.
Трудоемкость, з.е.	3
Форма отчетности	Экзамен, 2 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Расторгуев С.П. Основы информационной безопасности. – М.: Академия, 2014. – 192 с. 2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Академия, 2015. – 336 с. 3. Краковский Ю.М. Информационная безопасность и защита информации: Учебное пособие. – М.: ИКЦ «МарТ», Ростов н/Д: Издательский центр «МарТ», 2015. – 288 с.
Дополнительная литература	1. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ "Интернет-университет Информационных технологий", 2015. – 208 с. 2. Стандарты информационной безопасности: курс лекций: учебное пособие / Второе издание / В.А. Галатенко. Под редакцией академика РАН В.Б. Бетелина / – М.: ИНТУИТ.РУ "Интернет-университет Информационных технологий", 2014. – 264 с. 3. Соколов А. В., Степанюк О. М. Методы информационной защиты объектов и компьютерных сетей. – М.: АСТ, 2013.