

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:
 b47f96eea63a2dc27b994ab71b0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Защита информации от утечки по техническим каналам
Содержание	Общие вопросы технической защиты информации ограниченного доступа. Угрозы утечки информации по техническим каналам. Методы, способы и средства защиты информации от утечки по техническим каналам. Методы, способы и средства оценки защищенности информации от утечки по техническим каналам. Защита информации от несанкционированного доступа. Организация и обеспечение работ по технической защите информации. Аттестация, сертификация и лицензирование деятельности по технической защите конфиденциальной информации.
Реализуемые компетенции	ПК-10. Способен проводить аттестацию объектов вычислительной техники на соответствие требованиям по защите информации. ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.
Результаты освоения дисциплины (модуля)	ПК-10 Знать: 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. Уметь: 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. ОПК-5 Знать: 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: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации. Владеть: методами и средствами технической защиты информации. ОПК-9 Знать: технические каналы утечки информации; возможности технических средств перехвата информации; знает основные характеристики сигналов электросвязи, спектры и виды модуляции; Уметь: пользоваться нормативными документами в области технической защиты информации. Владеть: подходами к разработке и анализу безопасности криптографических протоколов. ОПК-13 Знать: технические каналы утечки информации; возможности технических средств перехвата информации; 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; основы физической защиты объектов информатизации. Уметь: пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта. Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.
Трудоёмкость, з.е.	4
Формы отчётности (в т.ч. по семестрам)	Экзамен, 7 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	Хорев, А.А. Защита информации от утечки по техническим каналам: учебное пособие / А.А Хорев – Защита информации от утечки по техническим каналам, 2006 – М.: МО РФ.
Дополнительная литература	Зайцев А.П. Технические средства и методы защиты информации: учебник для вузов /А.П. Зайцев / А.А. Шелупанов/ Р.В. Мещеряков – Технические средства и методы защиты информации 2012 – М.: Горячая линия – Телеком.