

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:
 b47f96eea65a20e27594abf1bb0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Программно-аппаратные средства защиты информации
Содержание	<p>Исследование корректности систем защиты. Реализация функциональных требований к системам анализа защищенности автоматизированных систем. Установка и настройка программно-аппаратных средств защиты от несанкционированного доступа. Программно-аппаратные средства анализа безопасности СВТ. Программно-аппаратные средства анализа безопасности передачи данных в локальных сетях. Программно-аппаратные средства анализа безопасности механизма авторизации СВТ. Программно-аппаратные средства анализа безопасности локального программного обеспечения СВТ. Программно-аппаратные средства анализа безопасности антивирусной защиты СВТ. Программно-аппаратные средства анализа безопасности в области противодействия методам социальной инженерии. Средства анализа безопасности беспроводной связи. Этап постэксплуатации тестирования на проникновение СВТ. Исследование механизмов защиты программ от незаконного использования и копирования. Исследование механизмов защиты программ от изучения и изменения. Установка и настройка штатных средств операционных систем, предназначенных для защиты от НСД и программно-аппаратных комплексов защиты от НСД. Установка и настройка программно-аппаратных средств защиты от НСД. Установка и настройка средств разграничения доступа и криптографической защиты информации. Установка и настройка средств контроля целостности защищаемых ресурсов и создания замкнутой программной среды. Установка и настройка межсетевых экранов, программно-аппаратных средств защиты информации при передаче по открытым каналам связи и разграничения доступа к сетевым ресурсам. Установка и настройка программно-аппаратных средств обнаружения сетевых атак и защиты от них. Испытание СВТ на соответствие требованиям по защите информации от несанкционированного доступа.</p>
Реализуемые компетенции	<p>ПК-3. Способен проводить сертификацию программно-аппаратных средств защиты информации и анализ результатов.</p> <p>ПК-10. Способен проводить аттестацию объектов вычислительной техники на соответствие требованиям по защите информации.</p>
Результаты освоения дисциплины (модуля)	<p>ПК-10</p> <p>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</p>

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.

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

	<p>защите информации; организационные меры по защите информации.</p> <p>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.</p> <p>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.</p>
Трудоемкость, з е	4
Форма отчетности	Экзамен, 4 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	<ol style="list-style-type: none"> 1. Программно-аппаратные средства защиты информационных систем: учебное пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков; Министерство образования и науки Российской Федерации; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. - 194 с.: ил. – http://biblioclub.ru/. – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6, экземпляров неограниченно 2. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации Электронный ресурс / сост. И. А. Денисов. – Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации, 2022-04-04. – Москва: Московский технический университет связи и информатики, 2016. – 31 с. – Книга находится в премиум-версии ЭБС IPR BOOKS. – ISBN 2227-8397, экземпляров неограниченно
Дополнительная литература	<ol style="list-style-type: none"> 1. Платонов, В. В. Программно-аппаратные средства защиты информации: учебник для вузов / В.В. Платонов. – Москва: Академия, 2013. – 330, [1] с.: ил.; 22. – (Высшее профессиональное образование. Информационная безопасность. Бакалавриат). – Библиогр.: с. 326-327. – ISBN 978-5-7695-9327-7, экземпляров 15 2. Программно-аппаратные средства обеспечения информационной безопасности, практикум, Душкин А.В., Барсуков О.М., Кравцов Е.В., 2019.