

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Программно-аппаратные средства защиты информации»

Дисциплина «Программно-аппаратные средства защиты информации» является частью программы бакалавриата «Информационная безопасность (общий профиль, СУОС)» по направлению «10.03.01 Информационная безопасность».

Цели и задачи дисциплины

формирование компетенций в области разработки и эксплуатации программно-аппаратных средств, используемых для обеспечения информационной безопасности автоматизированных систем.

Изучаемые объекты дисциплины

виды и классификация программных и аппаратных средства защиты автоматизированных систем; модели данных, систем и процессов защиты информации; угрозы безопасности информации в автоматизированных системах; схемы аутентификации в автоматизированных системах, использующие программные и аппаратные средства; методы и модели генерации и управления ключами; методы интеграции программных и аппаратных средства защиты в информационные системы; методы и средства обнаружения и предотвращения вторжений; средства антивирусной защиты в автоматизированных системах; методы построения виртуальных сетей в автоматизированных системах; методы, способы и средства обеспечения отказоустойчивости программных и аппаратных комплексов.

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		7	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	54	54	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	24	24	
- лабораторные работы (ЛР)			
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	54	54	
2. Промежуточная аттестация			
Экзамен			
Дифференцированный зачет			
Зачет	9	9	
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	108	108	

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
7-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Средства обеспечения информационной безопасности распределенных информационных систем	8	0	12	14
<p>Виртуальные среды и машины: уровень интеграции виртуальной системы и совместное использование ресурсов хост-машины. Кластеры. Облачные технологии SaaS, PaaS, IaaS и прочие. Размещение вычислительных ресурсов организации в коммерческих и свободных облачных хостингах.</p> <p>Экономические и правовые вопросы использования облачных технологий. Вопросы безопасности данных в виртуальных и облачных средах. Виртуальные частные сети (VPN). Программные и аппаратные средства создания VPN и VLAN</p> <p>Аппаратные криптошлюзы Континент и Криптон. Доступ удаленного пользователя в локальную сеть организации. Связь разбросанных филиалов организации в единую сеть. Организация межкорпоративного сетевого портала для ведения совместного проекта.</p> <p>Защищенный серфинг. криптографическая защита данных, передаваемых по каналам связи сетей общего пользования между составными частями VPN. Настройка приоритетов трафика. Маршрутизация трафика. Протоколирование сетевой активности. Блокировка трафика.</p> <p>Аудит автоматизированных информационных систем. Журналы событий в операционных системах, базах данных. Обеспечение доступности и надежного хранения корпоративных данных: резервное копирование и отказоустойчивые дисковые массивы RAID. Организация хранилища данных с использованием технологий NAS, SAN.</p>				
Безопасность сетевых автоматизированных систем	8	0	8	20
Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Программно-аппаратные средства аутентификации:				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
<p>биометрические, пассивные и активные устройства. Сетевая аутентификация в корпоративных системах. Управление сертификатами Kerberos. Протокол LDAP. Инфраструктура управления ключами PKI. Принципы работы и функционал СЗИ. Обеспечение безопасной загрузки операционной системы и верификация модулей. Централизованное управление. Интеграция в существующую автоматизированную систему предприятия. Средства, сертифицированные ФСТЭК. Примеры СЗИ</p> <p>Структура и функционал электронных ключей. Программные модули: драйвер ключа и API ключа. Структура защищенной программы. Преимущества и ограничения ключей как методы защиты ПО от нелегального распространения. Виды защиты: конверт (envelope), триальные и ограниченные версии, интеграция API ключа в разрабатываемую программу.</p> <p>Разрушающие программные воздействия: вирусы, трояны, malware, adware.</p> <p>Классификация и технологии вирусов.</p> <p>Руткиты: вредоносное ПО для организации удаленного управления ЭВМ и создания ботнетов</p> <p>IDS/IPS. Алгоритмы интеллектуального анализа сетевой и локальной активности, выявляющие нестандартный обмен информацией. Пассивное и активное обнаружение атак. Примеры систем предотвращения вторжений: Microsoft TMG, Snort.</p>				
Безопасность локальных вычислительных систем	8	0	8	20
<p>Предмет и задачи программно-аппаратной защиты информации. Автоматизированная система (АС). Структура и компоненты АС. Сети ЭВМ. Электронный документ (ЭД). Виды информации в КС. Информационные потоки в КС. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Политика безопасности в компьютерных системах.</p>				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
<p>Оценка защищенности. Способы защиты конфиденциальности, целостности и доступности в КС. Стандарты и рекомендации по оценке защищенности от НСД</p> <p>Архитектура ЭВМ и виды современных многопользовательских и многозадачных операционных систем. Реализация подсистемы безопасности ОС. Идентификация и аутентификация пользователей ОС</p> <p>Контроль доступа и разграничение доступа. Дискреционное и мандатное разграничение доступа. Пользователи и группы. Файл как объект доступа. Оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости. Иерархический доступ к файлу. Понятие атрибутов доступа. Защита файловых ресурсов в ОС Windows и Unix</p> <p>Способы исследования программ, виды отладчиков. Ресурсы, упакованные в программном модуле. Секции программ. Трассировка программ платформы Win32 и программ, платформ .NET и Java</p>				
ИТОГО по 7-му семестру	24	0	28	54
ИТОГО по дисциплине	24	0	28	54