МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

«Системы обнаружения компьютерных атак»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____/В.И. Белоножкин/

Заведующий кафедрой
Систем информационной
безопасности _____/ А.Г. Остапенко /

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Формирование и закрепление общепрофессиональных и профессиональных компетенций, направленных на знание и владение современными методами и технологиямиобнаружения и отражения компьютерных атак

1.2.Задачиосвоениядисциплины

- ознакомление с основными принципами построения систем обнаружения компьютерных атак, способах обнаружения и нейтрализации последствий вторжений в компьютерные системы;
- формирование умений анализировать защищенность компьютерных систем, администрировать системы обнаружения компьютерных атак;
- приобретение навыков выявления и устранения уязвимостей компьютерных систем, настройки систем обнаружения компьютерных атак.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Системыобнаружениякомпьютерныхатак»относитсякдисциплинамбазовойчастиблокаБ1.Данная программа строится на преемственности программ в системе высшего образования и предназначена для студентов ФГБОУ ВПО «ВГТУ». Для освоения дисциплины "Системы обнаружения компьютерных атак" требуются знания и умения, приобретенные обучающимися в результате освоения ряда предшествующих дисциплин (разделов дисциплин), таких как: информатика, высшая математика,

Программа устанавливает минимальные требования к знаниям и умениям студентов, обучающихся по направлению 10.05.01 «Компьютерная безопасность», специализация "Безопасность распределённых компьютерных систем" и определяет содержание и виды учебных занятий и отчетности.

Программа разработана в соответствии с: Федеральным государственным образовательным стандартом по направлению подготовки 10.05.01 «Компьютерная безопасность»; Основной профессиональной образовательной программой и учебным планом по направлению подготовки 10.05.01 «Компьютерная безопасность», специализация "Безопасность распределённых компьютерных систем".

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизученидисциплины«Системыобнаружениякомпьютерныхатак»направленаформированиеследующихкомпетенций:

ОПК-3-

способностьюпониматьзначениеинформациивразвитиисовременногообщества,применятьдостиженияинформационныхтехнологийдляпоискаиобработкиинформациипопрофилюдеятельностивглобальныхкомпьютерныхсетях,библиотечныхфондахиныхисточникахинформации

ПК-7-

способностьюпроводитьанализпроектныхрешенийпообеспечениюзащищенностикомпьютерныхсистем

ПК-16-способностьюразрабатыватьпроектынормативныхправовыхактовиметодическиематериалы,регламентирующиеработупообеспечениюинформационнойбезопасностикомпьютерныхсистем

ПК-20-способностьювыполнятьработыповосстановлениюработоспособностисредствзащитыинформациипривозникновенииинештатныхситуаций

ПСК-3.2-способностьюанализироватьзащитуинформациираспределенныхкомпьютерныхсистемах,проводитьмониторинг,аудитиконтрольныепроверкиработоспособностиизащищенностираспределенныхкомпьютерныхсистем

ПСК-3.3-способностьюиспользоватьсовременныесредыитехнологии,разработкипрограммногообеспечениявраспределенныхкомпьютерныхсистемахсучетомтребованийинформационнойбезопасности

Компетенция	**Результатыобучения,характеризующие сформированностькомпетенции**
ОПК-3	знать основные направления и тенденции развития информационной сферы
	уметь находить, систематизировать ианализировать информацию из различных источников
	владеть навыками эффективного применения программных средств, используемых в современных поисковых системах
ПК-7	знать основные принципы построения защищенных распределенных компьютерных систем
	уметь анализировать защищенность компьютерныхсистем
	владеть навыками выявления и устранения уязвимостей компьютерных систем
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак
	уметь формализовать задачу управления безопасностью компьютерных систем
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем
ПК-20	знать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы
	уметь администрировать системы обнаружения компьютерных атак
	владеть навыками организации защищенного

	удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак
ПСК-3.2	знать направления и методы анализа защищенности компьютерных систем
	уметь применять методики и инструментыанализа защищенности компьютерных систем
	владеть навыками управления средствами мониторинга и аудита компьютерных систем
ПСК-3.3	знать направления и тенденции развития безопасных информационных технологий
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Системыобнаружениякомпьютерныха так»составляет7з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Виды учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	108	54	54
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	36	18	18
Самостоятельная работа	108	72	36
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 126 3.5	 126 3.5

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостипо видамзанятий

очнаяформаобучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Системный подход к обес-печению защиты	Компьютерные системыи их компоненты как объекты защиты от угроз безопасности.	24	10	40	74

	от компью-терных атак	Направления, методы и методики построения защищенных компьютерных систем. Организационные методы и средства защиты компьютерных систем от атак.				
2	Средства выявления и локализа-ции уязви-мостей компью-терных си-стем к воз-действию угроз без-опасности	Методы и средства оценки защищенности, контроля доступа к компонентамкомпьютерных систем. Методы и средства обеспечения безопасности электропитания компьютерных систем, гарантированного уничтожения информации, выявления и локализации утечек информации по техническим каналам	12	8	32	52
3	Методы и средства обнаруже-ния и отра-жения се-тевых атак	Методы и средства обнаружения сетевых атак и вредоносных программ. Контентная фильтрация и межсетевое экранирование. Средства создания виртуальных частных сетей.	18	10	18	46
4	Комплекс-ные системы защиты от компью-терных атак	Доверенные аппаратные среды. Подсистемы безопасности операционных систем, СУБД, прикладного программного обеспечения. Комплексные системы защиты локальных и корпоративных сетей. Системы контроля работы пользователей компьютерных систем. Оснащение центров Государственной системы обнаружения и противодействия компьютерным атакам РФ.	18	8	18	44
		Итого	**72**	**36**	**108**	**216**

5.2Перечьлабораторныхработ

Непредусмотреноучебнымпланом

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматривает выполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-3	знать основные направления и тенденции развития информационной сферы	Ответ на вопрос преподавателя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь находить, систематизировать ианализировать информацию из различных источников	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками эффективного применения программных средств, используемых в современных поисковых системах	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-7	знать основные принципы построения защищенных распределенных компьютерных систем	Ответ на вопрос преподавателя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать защищенность компьютерных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками выявления и устранения уязвимостей компьютерных систем	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-16	знать основные	Ответ на вопрос	Выполнение работ в	Невыполнение

	принципы построения систем обнаружения компьютерных атак	преподавателя	срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
	уметь формализовать задачу управления безопасностью информационных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками проведения анализа рисков и администрировани я безопасности распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-20	знать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Ответ на вопрос преподавателя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь администрировать системы обнаружения компьютерных атак	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.2	знать направления и методы анализа защищенности компьютерных систем	Ответ на вопрос преподавателя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять методики и инструментыанализ а защищенности компьютерных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками управления средствами мониторинга и аудита компьютерных систем	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-3.3	знатьнаправления и тенденции развития	Ответ на вопрос преподавателя	Выполнение работ в срок,	Невыполнение работ в срок,

	безопасных информационных технологий		предусмотренный в рабочих программах	предусмотренный в рабочих программах
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв7,8семестредлячнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Критерии оценивания**	**Зачтено**	**Незачтено**
ОПК-3	знать основные направления и тенденции развития информационной сферы	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь находить, систематизировать ианализировать информацию из различных источников	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками эффективного применения программных средств, используемых в современных поисковых системах	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-7	знать основные принципы построения защищенных распределенных компьютерных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь анализировать защищенность компьютерных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками выявления и устранения уязвимостей компьютерных	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	систем			
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь формализовать задачу управления безопасностью информационных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками проведения анализа рисков и администрировани я безопасности распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-20	знать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь администрировать системы обнаружения компьютерных атак	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПСК-3.2	знать направления и методы анализа защищенности компьютерных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять методики и инструментыанализ а защищенности компьютерных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками управления средствами мониторинга и аудита компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

ПСК-3.3	знатьнаправления и тенденции развития безопасных информационных технологий	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	**Результатыобучения ,характеризующие сформированностьк омпетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-3	знать основные направления и тенденции развития информационной сферы	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь находить, систематизироват ь ианализировать информацию из различных источников	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонст р ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками эффективного применения программных средств, используемых в современных поисковых системах	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонст р ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-7	знать основные принципы построения защищенных распределенных компьютерных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь анализировать	Решение стандартных	Задачи решены в	Продемонст р ирован	Продемонстр ирован верный	Задачи не решены

	защищенность компьютерных систем	практических задач	полном объеме и получены верные ответы	верный ход решения всех, но не получен верный ответ во всех задачах	ход решения в большинстве задач	
	владеть навыками выявления и устранения уязвимостей компьютерных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь формализовать задачу управления безопасностью информационных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-20	знать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь администрироват ь системы обнаружения компьютерных атак	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками организации защищенного	Решение прикладных задач в конкретной	Задачи решены в полном объеме и	Продемонстр ирован верный ход решения	Продемонстр ирован верный ход решения в большинстве	Задачи не решены

	удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак	предметной области	получены верные ответы	всех, но не получен верный ответ во всех задачах	задач	
ПСК-3.2	знать направления и методы анализа защищенности компьютерных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь применять методики и инструментыанализа защищенности компьютерных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками управления средствами мониторинга и аудита компьютерных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.3	знатьнаправления и тенденции развития безопасных информационных технологий	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыков

и(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Компьютерная атака - это:

а) реализация угрозы безопасности;

б) целенаправленное воздействие на компьютерную систему программно-техническими средствами, направленное на нарушение доступности, целостности, конфиденциальности информации;

в) проявление уязвимости компьютерной системы.

2. Угрозы безопасности компьютерным системам могут быть классифицированы:

а) по направленности реализации

б) по типу уязвимости;

в) по способу устранения негативных последствий.

3. Завершающим этапом компьютерной атаки является:

а) получение несанкционированного доступа;

б) маскировка следов атаки;

в) планирование атаки

4. Уязвимость компьютерной системы- это:

а) свойство ее компонента или процесса, путем использования которого может быть осуществлено несанкционированное воздействие на объекты защиты;

б) проявление воздействия угрозы безопасности;

в) нарушение работы средств защиты информации.

5. К идентификационным признакам контроля доступа к компьютерным системам относятся:

а) биометрические характеристики;

б) паспортные жанные;

в) IP-адрес компьютера.

7. К основнымнаправлениям контроля эффективности ЗИ в КС относятся:

а) мониторинг работы пользователей;

б) моделирование компьютерных атак;

в) проверка журналов системных событий.

8. В состав функций средств обнаружения вторжений входит:

а) конфигурирование сетевых устройств;

б) контроль работы системного администратора;

в) выявление атак и подозрительной сетевой активности.

9. Сеть-приманка - это:

а) защищенный ресурс, который служит объектом атак;

б) атакуемый фрагмент корпоративно сети;

в) средство выявления утечек информации.

10. Корпоративный центр ГосСОПКА должен включать в себя:

а) удостоверяющий центр ЭЦП;

б) центр операций по обеспечению безопасности;

в) центр управления ключевой информацией.

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. К техническим характеристикам электронных замков относится:

а) быстродействие;

б) способ считывания информации;

в) компания-производитель.

2. Рекомендации по использованию программных СЗИ нужны для:

а) выбора оптимального состава СЗИ;

б) подготовки эксплуатационной документации;

в) организации работы службы информационной безопасности.

3. В архитектуру типовой комплексной СЗИ для локальных сетей входит:

а) рабочее место администратора;

б) подсистема шифрования трафика;

в) криптоядро.

4. В защищенной операционной системе базовые средства защиты располагаются в:

а) прикладных программах;

б) ядре;

в) системных службах.

5. Риск компьютерной атаки рассчитывается как:

а) сумма ущербов от реализованной атаки;

б) произведение вероятности реализации атаки и возможного ущерба ;

в) произведение рейтинга атаки и ее длительности.

6. DOS-атака нарушает:

а) конфиденциальность;

б) доступность;

в) своевременность.

7. Основное свойство компьютерного вируса:

а) уничтожение информации;

б) размножение;

в) скрытность.

8. Системы контроля пользователей применяются для:

а) выявления инсайдерских утечек информации;

б) мониторинга внешней сетевой активности;

в) подтверждения лояльности сотрудников.

9. Для обнаружения компьютерных атак используются:

а) наборы правил;

б) сигнатуры;

в) шаблоны и макросы.

10. В число отличий локальной и корпоративной сетей входит:

а) количество сетевых соединений;

б) вид сетевого протокола;

в) расположение линий связи относительно контролируемой зоны.

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Настройка веб-браузера для обеспечения безопасной работы в

Интернет включает в себя:

а) установку дополнений;

б) отключение всплывающих окон;

в) блокировку загрузки файлов.

2. Описание примерного алгоритма обнаружения атаки типа "отказ в обслуживании" начинается с:

а) формулировки задачи;

б) перечисления контролируемых портов;

в) поиска злоумышленника.

3. Разграничение доступа пользователей на основе дискреционного принципа контроля использует механизм:

а) ролей;

б) меток безопасности;

в) набора правил.

4. Функции управления СЗИ "Secret Net" разделяютя для:

а) пользователей сети;

б) сотрудников ИТ-службы;

в) администраторов безопасности.

5. Основные настройки персонального межсетевого экрана для обеспечения безопасной работы в Интернет регулируют:

а) входящий трафик;

б) отображение графики на экране;

в) количество запускаемых приложений.

6. Типовая структура подсистемы безопасности операционной системы включает в себя:

а) средства аутентификации;

б) сетевые драйверы;

в) модуль ввода-вывода.

7. Защищенная СУБД отличается наличием:

а) подсистемы безопасности;

б) средств шифрования;

в) сетевых служб.

8. Средства моделирования атак используют:

а) алгоритмы известных атак;

б) перебор случайных воздействий;

в) многократное повторение базовых оперций ввод-вывода.

9. К техническим характеристикам средств обнаружения и блокирования сетевых атак относится:

а) время реагирования;

б) наличие функции отключения;

в) нагрузочная способность.

10. Набор функций AAA для беспроводных сетей включает:

а) авторизацию;

б) ассоциацию;

в) атрибутизацию.

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Классификация угроз безопасности компьютерным системам.
2. Системные принципы защиты информации в компьютерных системах.
3. Стратегические направления государственной политики России в сфере противодействия компьютерным атакам
4. Методика построения комплексной защиты компьютерных систем.
5. Информационные технологии, повышающие защищенность компьютерных систем.
6. Структура и функции ГосСОПКА.
7. Методика расследования компьютерных атак
8. Характеристика средств защиты целостности и бесперебойности функционирования компьютерных систем.
9. Методика организации защищенного электропитания компьютерных систем.
10. Методы и средства контроля эффективности защиты информации в компьютерных системах.

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Описать алгоритм проведения атаки, направленной на получение НСД к информации КС через Интернет
2. Предложить обоснованное решение для организации контроля доступа к компьютеру нескольких пользователей с разными правами
3. Сделать ориентировочный расчет рисков для системы электронной почты коммерческой организации с трехуровневой системой оценки вероятностей и ущерба от реализации угроз.
4. Построить схему включения источников бесперебойного электропитания для КС, состоящей из 2 серверов и 5 рабочих станций с возможностью автоматического останова-запуска центрального узла сети
5. Обосновать выбор средств контроля доступа в помещение серверной объекта критической инфраструктуры.
6. Проранжировать способы удаления информации с компьютерных носителей по степени надежности и стоимости.
7. Дать обоснованные рекомендации по использованию средств обеспечения конфиденциальности в иерархической локальной сети.
8. Построить схему включения межсетевых экранов в сетевой структуре с наличием корпоративного веб-сервера и интернет-сайта при условии обеспечения доступа внутренних пользователей к обоим ресурсам.
9. Сформулировать правила разграничения доступа к ресурсам сервера организации, два подразделения которой обрабатывают изолированную друг от друга информацию.
10. Определить состав и количество компонентов системы защиты корпоративной сети, включающей 3 удаленных сегмента, 50 пользовательских компьютеров и 4 сервера.

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточнойаттестации

Зачетпроводитсяпотест-билетам,каждыйизкоторыхсодержит5вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,верное решение адачиоценивается в 5баллов.Максимальноеколичествонабранныхбаллов–10.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее2баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот2до4баллов.

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот5до7баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот8до10баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы) дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочного средства
1	Системный подход к обеспечению защиты от компьютерных атак	ОПК-3, ПК-7, ПК-16, ПК-20, ПСК-3.2, ПСК-3.3	Тест, контрольная работа, защита реферата
2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз безопасности	ОПК-3, ПК-7, ПК-16, ПК-20, ПСК-3.2, ПСК-3.3	Тест
3	Методы и средства обнаружения и отражения сетевых атак	ОПК-3, ПК-7, ПК-16, ПК-20, ПСК-3.2, ПСК-3.3	Тест, защита реферата
4	Комплексные системы защиты от компьютерных атак	ОПК-3, ПК-7, ПК-16, ПК-20, ПСК-3.2, ПСК-3.3	Тест

7.3.Методическиематериалы,определяющиепроцедурыоцениванияознаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменаторомивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпр

оведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

1. Лукацкий А.В. Обнаружение атак, 2003, Печат.
2. Стивен Норткатт и др. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу, 2001, Печат.
3. Мак-Клар С. Хакинг в Web: атаки и защита, 2003, Печат.
4. Шелухин О.И. и др. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие, 2013, Печат.

Шелухин, О.И.
Системы обнаружения вторжений в компьютерные сети [Электронный ресурс] : учебное пособие / А.В. Савелов; А.Н. Руднев; О.И. Шелухин. - Системы обнаружения вторжений в компьютерные сети ; 2022-04-04. - Москва : Московский технический университет связи и информатики, 2013. - 88 с. URL: http://www.iprbookshop.ru/63360.html

5. Остапенко А.Г. Теория сетевых войн, 2015, Эл.ресурс.
6. Остапенко А.Г. Сетевое противоборство социотехнических систем2015, Эл.ресурс.
7. Остапенко А.Г. и др. Эпидемии в телекоммуникационных сетях, 2018, Печат.
8. Чирилло Дж. Обнаружение хакерских атак. Для профессионалов, 2002, Печат.
9. Белоножкин В.И Автоматизированные защищенные системы: учеб. пособие, 2014, Эл.ресурс.
10. Белоножкин В.И., Системы обнаружения компьютерных атак (учебное пособие), 2015, Эл.ресурс.
11. Кулаков В.Г. и др. Моделирование информационных операций и атак в сфере государственного и муниципального управления (монография), 2004, Печат.
12. Шумский А.А, .Шелупанов А. А. Системный анализ в защите информации, 2005, Печат.
13. Локхарт Э. Антихакинг в сети, 2005, Печат.
14. Остапенко Г.А., Радько Н.М. и др. Модели обнаружения сетевых вторжений : учеб.пособие, 2013, Эл.ресурс.

8.2Переченьинформационныхтехнологий,используемыхприосуществлении образовательногопроцессаподисциплине,включаяперечень лицензионного программногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

–Электронный журнал "*Информационная безопасность*", http://www.itsec.ru
–Электронный ресурс "Безопасность информационных систем", http://infobez.com
–Портал "Центр информационной безопасности" http://www.bezpeka.com/ru
–Портал «Anti-Malware» https://www.anti-malware.ru
–операционные системыMicrosoft Windows, Linux;
–офисное ПО «Libre Office»
–СУБД «Линтер»;

– СПО «Secret Net»;
– СПО «Vipnet client»;
– антивируное ПО «Kaspersky free”.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРА

ЗОВАТЕЛЬНОГОПРОЦЕССА

Аудитория с компьютерными рабочими местами, локальная сеть, презентационное оборудование.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Системыобнаружениякомпьютерныхатак»читаютсялекции,проводятсяпрактическиезанятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотраженияв учебнойлитературе.

Практическиезанятиянаправленынаприобретениепрактическихнавыковиспользования методов и средств выявления и локализации последствий компьютерных
атак.Занятияпроводятсяпутемрешенияконкретныхзадачваудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.