МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.06 Безопасность информационно-аналитических систем

1. Код и наименование направления подготовки/специальности:
10.05.04 Информационно-аналитические системы безопасности

2. Профиль подготовки/специализация: "Автоматизация информационно-аналитической деятельности", "Информационная безопасность финансовых и экономических структур"

3. Квалификация выпускника: специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: математического анализа

6. Составители программы:
Найдюк Филипп Олегович, канд. физ.-мат. наук, доцент кафедры математического анализа

7. **Рекомендована:** Научно-методическим Советом математического факультета, протокол **№0500-07 ОТ 29.06.2021**.

8. Учебный год: 2024/2025 **Семестр:** 8

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:
- сущность и понятие информации, информационной безопасности и характеристика её составляющих;
- источники и классификация угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- основные виды и угрозы безопасности операционных систем;
- основные стандарты в области инфокоммуникационных систем и технологий;
- защитные механизмы и средства обеспечения сетевой безопасности;
- средства и методы предотвращения и обнаружения вторжений;
- основные отечественные и зарубежные стандарты в области компьютерной безопасности;
- основные методы организационного обеспечения информационной безопасности специальных ИАС;

Задачи учебной дисциплины:
- уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- уметь применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- пользоваться средствами защиты, предоставляемыми системами управления базами данных;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- владеть навыками безопасного использования технических средств в профессиональной деятельности;
- владеть методами и средствами выявления угроз безопасности компьютерным системам.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Безопасность информационно-аналитических систем» относится к учебным дисциплинам обязательной части блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

Дисциплина «Безопасность информационно-аналитических систем» базируется на знаниях, полученных по дискретной математике, информатике и численным методам.

Приобретенные в результате обучения знания, умения и навыки используются в рамках последующих предметов:

- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;

- информационно-аналитические системы.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-6.2	Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - основные методы организационного обеспечения информационной безопасности специальных ИАС; - назначение и классификацию информационных и аналитических систем, систем управления уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; пользоваться средствами защиты, предоставляемыми системами управления базами данных; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем владеть: - навыками моделирования технологических процессов обработки информации в специальных ИАС с заданной степенью статистической надежности результатов; - навыками исследования математических моделей технологических процессов обработки информации в специальных ИАС с целью оценки качества и оптимизации характеристик специальных ИАС
ОПК-11.2	Способен разрабатывать систему защиты информации информационно-	знать: - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения

	аналитических систем	информационной безопасности, принципы построения систем защиты информации; - основные виды и угрозы безопасности операционных систем; - защитные механизмы и средства обеспечения сетевой безопасности; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - основные методы организационного обеспечения информационной безопасности специальных ИАС уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - решать задачи исследования специальных ИАС методами моделирования; - применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных ИАС; - решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных владеть: - навыками безопасного использования технических средств в профессиональной деятельности
ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; защитные механизмы и средства обеспечения сетевой безопасности; - принципы эксплуатации и сопровождения ИАС; - средства и методы предотвращения и обнаружения вторжений уметь: - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - проектировать и сопровождать типовые специальные ИАС, локальные сети; - применять отечественные и зарубежные

		стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем владеть: - методами и средствами выявления угроз безопасности компьютерным системам; - методами моделирования безопасности компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах; - простейшими методами анализа безопасности криптографических протоколов

12. Объем дисциплины в зачетных единицах/час. — 4/144.

Форма промежуточной аттестации зачёт с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра: 7	№ семестра: 8	…
Аудиторные занятия		64		64	
в том числе:	лекции	32		32	
	практические				
	лабораторные	32		32	
Самостоятельная работа		80		80	
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачёт с оценкой)*					
Итого:		144		144	

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
Лекции			
1.1	Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ.	Исторические моменты формирования ИБ. Составляющие информационной безопасности. Доктрина информационной безопасности РФ. Общая структура ИБ. Требования по обеспечению	–

		ИБ. Классификация защиты информации. Ранжирование ИТ-угрозы. Спецификация полей ИБ.	
1.2	Виды угроз ИБ и методы их анализа.	Критерии классификации угроз ИБ. Модели. Алгоритмы анализа угрозы и оценки ИБ. Основные виды защищаемой информации.	–
1.3	Правовое обеспечение ИБ	Российское законодательство в области ИБ: законы, постановления и другие нормативные акты.	–
1.4	Построение системы ИБ	Уровни программы информационной безопасности. Математические модели в реализации концепции и программы ИБ. Системы защиты информации (СЗИ). Генетический алгоритм. Анализ и управление рисками при реализации ИБ. Защита информации в информационных системах и компьютерных сетях.	–
1.5	Информационные системы (ИС) и обеспечение их безопасности	Трёхуровневая модель оценки защищённости ИС. Требования к архитектуре ИС. Стандарты. Технологии криптографической защиты информации. Межсетевые экраны. Защищённые виртуальные сети VPN. Антивирусная защита. Классификация угроз ИС: сетевые черви, вирусы, троянские программы и прочие вредоносные утилиты.	–
1.6	Создание архитектуры информационно-аналитических систем (ИАС)	Аналитические системы: процессы и инструменты. Описание общей структуры. Степени ИБ. Особенности применения и анализа информации.	–
Лабораторные работы			
2.1	Методы анализа угроз ИБ	Алгоритмы анализа угрозы и оценки ИБ. Классификация основных видов защищаемой информации.	–
2.2	Построение системы ИБ	Математические модели в реализации концепции и программы ИБ. Использование систем защиты информации (СЗИ). Генетический алгоритм. Построение защиты информации в информационных системах и компьютерных сетях.	–
2.3	Информационные системы (ИС) и обеспечение их	Создание и анализ трёхуровневой модели оценки защищённости ИС.	–

	безопасности	Эксплуатация межсетевых экранов. Технологии криптографической защиты информации. Оценка защищённости виртуальных сетей VPN. Антивирусная защита. Классификация угроз ИС	
2.4	Создание архитектуры ИАС	Использование аналитических систем. Создание общей структуры по степеням ИБ	–

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ.	2		2	2	6
02	Виды угроз ИБ и методы их анализа.	4		2	10	16
03	Правовое обеспечение ИБ	2			14	16
04	Построение системы ИБ	8		10	20	38
05	Информационные системы (ИС) и обеспечение их безопасности.	8		8	16	32
06	Создание архитектуры информационно-аналитических систем (ИАС)	8		10	18	36
Итого		32		32	80	144

14. Методические указания для обучающихся по освоению дисциплины:

В процессе освоения дисциплины студенты должны посетить лекционные и лабораторные занятия и сдать зачёт на оценку.

Указания для освоения теоретического и практического материала и сдачи зачёта:

1. Обязательное посещение лекционных и лабораторных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.

3. Копирование (электронное) перечня вопросов к экзамену по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.

4. При подготовке к лабораторным занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.

5. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет – поиск информации по ключевым словам курса (видеофайлов, файлов-презентаций, файлов с учебными пособиями) и ознакомиться с найденной информацией при подготовке к зачёту по дисциплине.

Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала с разбором основных типовых задач, имеется зачёт по контрольной работе.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	***Голуб, В. А**. Информационная безопасность компьютерных систем. Защита целостности информации / В.А. Голуб. – Воронеж: ЛОП ВГУ, 2006.– 31 с.*
2	***Девянин, П. Н.** Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П.Н. Девянин. – Москва: Горячая линия-Телеком, 2017. – 338 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111049*
3	***Пугин, В. В.** Защита информации в компьютерных информационных системах / В.В. Пугин, Е.Ю. Голубничая, С.А. Лабада. – Самара: ПГУТИ, 2018. – 119 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/182299*

б) дополнительная литература:

№ п/п	Источник
4	***Астанин, И. К**. Защита информации / И.К. Астанин, Н.И. Астанин.– Воронеж: Воронеж. гос. ун-т, 2006.– с.169*
5	***Галицкий, А. В**. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин.– М.: ДМК Пресс, 2004.– 613 с.*
6	***Мельников, В. П**. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков.– М.: ACADEMIA, 2006.– 330 с.*
7	***Гайдамакин, Н. А**. Автоматизированные информационные системы, базы и банки данных / Н.А. Гайдамакин.– М.: Гелиос АРВ, 2002.– 367 с.*
8	***Мизин, И.А.** Автоматизированные системы управления. Основы теории информационных систем / И.А. Мизин, Л.С. Уринсон, Г.К. Храмешин; Московский институт радиотехники, электроники и автоматики.– М., 1971.– 173 с.*
9	***Ярочкин, В. И.** Безопасность информационных систем / В. И. Ярочкин.– М.: Ось-89, 1996.– 318 с.*
10	***Круглов, В. В**. Интеллектуальные информационные системы: Компьютерная поддержка систем нечеткой логики и нечеткого вывода / В.В. Круглов, М.И. Дли.– М.: Физматлит, 2002.– 254 с.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
11	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
12	*Электронно-библиотечная система "Консультант студента". –*

	(http://www.studentlibrary.ru/)
13	*Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)*
14	*Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	***Алдохина, О.И.*** *Информационно-аналитические системы и сети / О.И. Алдохина. – Кемерово: КемГИК, – 2010. – 148 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/49636*
2	***Прокопенко, Н.Ю.*** *Аналитические информационные системы поддержки принятия решений / Н. Ю. Прокопенко. – Нижний Новгород: ННГАСУ, 2020. – 142 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/164866*
3	*Официальный сайт компании «BaseGroup Labs» [Электронный ресурс]. Рязань, 1995-2010.- Режим доступа: http://www.basegroup.ru/*

Курс дисциплины построен таким образом, чтобы позволить студентам проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается интерактивный диалог с преподавателем, осуществляемый с помощью удаленной связи через интернет на платформе образовательного портала «Электронный университет ВГУ».

Самостоятельная работа студента, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый на лекции и в ходе лабораторных работ. Необходимо овладеть навыками библиографического поиска, уметь находить подходящие источники, творчески и критически перерабатывать информацию, научиться определять методы исследований.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины проводятся различные типы лекций (вводная, обзорная и т.д.).

При осуществлении самостоятельной работы возможна интерактивная связь с преподавателем через сеть интернет на платформе образовательного портала «Электронный университет ВГУ». Проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО на системах с ОС: Windows 10 и Ubuntu 20.04.

18. Материально-техническое обеспечение дисциплины:

Учебные аудитории для проведения лекционных и практических занятий. Компьютерные классы для выполнения индивидуальных заданий, оснащённые лицензионным и свободно распространяемым программным обеспечением: Windows 10, Ubuntu 20.04, Linux, информационно-аналитическая платформа Loginom, Deductor (Academic), программное обеспечение для виртуализации персонального компьютера Oracle VM VirtualBox, снифер Wireshark, система обнаружения атак Suricata. В ходе

лабораторных занятий задействуется учебно-лабораторный стенд «Сетевая безопасность».

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	Оценочные средства
ОПК-6.2: Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - источники и классификацию угроз информационной безопасности; -основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - основные методы организационного обеспечения информационной безопасности специальных ИАС; - назначение и классификацию информационных и аналитических систем,	01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ; 04, Построение системы ИБ	Устный опрос

	систем управления		
	уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; пользоваться средствами защиты, предоставляемыми системами управления базами данных; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС)	Устный опрос
	владеть: - навыками моделирования технологических процессов обработки информации в специальных ИАС с заданной степенью статистической надежности результатов; - навыками исследования математических моделей технологических процессов обработки информации в специальных ИАС с целью оценки качества и оптимизации характеристик специальных ИАС	04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности; 06, Создание архитектуры информационно-аналитических систем (ИАС)	Практическое задание
ОПК-11.2: Способен разрабатывать систему защиты информации информационно-аналитических систем	знать: - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем	01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ; 06, Создание архитектуры	Устный опрос

	защиты информации; - основные виды и угрозы безопасности операционных систем; - защитные механизмы и средства обеспечения сетевой безопасности; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности; - основные методы организационного обеспечения информационной безопасности специальных ИАС	информационно-аналитических систем (ИАС)	
	уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; -решать задачи исследования специальных ИАС методами моделирования; - применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных ИАС; - решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных	01, Понятия информационной безопасности (ИБ); 02, Виды угроз ИБ и методы их анализа; 04, Построение системы ИБ; 05, Информационные системы (ИС) и обеспечение их безопасности	Устный опрос
	владеть: - навыками безопасного использования технических средств в	Виды угроз ИБ и методы их анализа; 03, Правовое обеспечение ИБ;	Практическое задание

	профессиональной деятельности	04, Построение системы ИБ; 06, Создание архитектуры информационно-аналитических систем (ИАС)	
ОПК-13.4: Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	знать: - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; защитные механизмы и средства обеспечения сетевой безопасности; - принципы эксплуатации и сопровождения ИАС; - средства и методы предотвращения и обнаружения вторжений	02, Виды угроз ИБ и методы их анализа	Устный опрос
	уметь: - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - проектировать и сопровождать типовые специальные ИАС, локальные сети; - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	02, Виды угроз ИБ и методы их анализа	Устный опрос
	владеть: - методами и средствами выявления угроз безопасности компьютерным системам; - методами моделирования безопасности	02, Виды угроз ИБ и методы их анализа	Практическое задание

	компьютерных систем, в том числе, моделирования управления доступом и информационными потоками в компьютерных системах; - простейшими методами анализа безопасности криптографических протоколов		

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- Тестовые задания;
- Лабораторные работы;
- Контрольная работа.

Примерный перечень заданий проверки практических навыков

1. Привести пример действия атакующего и способ защиты от атаки «man-in-the-middle».
2. Привести пример структуры и функциональности стека протоколов TCP/IP.
3. Применить алгоритм кластеризации по заданной модели.
4. Подсчитать метрику релевантности информационного сообщения по данным профиля и микроблога конкретного пользователя сети.
5. Определить скорость распространения информации по имитационной модели распространения информации в социальной сети на выбор (SIS. SIR, SIDR).
6. Рассчитать среднее значение кластерного коэффициента для большого графа программным методом.
7. Создать класс-обёртку для вызова API функций социальных сетей.
8. Провести ROC-анализ на заданной регрессионной модели.
9. Описать методы функции Data Mining.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- Собеседование по билетам к зачету (с оценкой).

Примерный перечень вопросов к зачёту

1. Основные понятия защиты информации и информационной безопасности.
2. Анализ угроз информационной безопасности.
3. Модель ISO/OSI и стек протоколов TCP/IP.
4. Проблемы безопасности IP-сетей.

5. Угрозы и уязвимости проводных корпоративных сетей.
6. Угрозы и уязвимости проводных беспроводных сетей.
7. Способы обеспечения информационной безопасности.
8. Пути решения проблем защиты в информационных сетях.
9. Структура политики безопасности.
10. Базовая политика безопасности.
11. Специализированные политики безопасности.
12. Процедуры безопасности.
13. Стандарты информационной безопасности и их роль.
14. Стандарты ISO/IEC 17799:2002.
15. Стандарт BS1 (Германия).
16. Международный стандарт ISO 15408.
17. Стандарты безопасности беспроводных сетей.
18. Стандарты информационной безопасности в Интернете.
19. Стандарты безопасности информационных технологий РФ.
20. Основные понятия криптографии.
21. Симметричные криптосистемы шифрования.
22. Асимметричные криптосистемы шифрования.
23. Комбинированная криптосистема шифрования.
24. Основные процедуры цифровой подписи.
25. Управление USB-ключами eToken.
26. Классификация криптографических алгоритмов.
27. Основные методы аутентификации.
28. Межсетевой экран. Фильтрация трафика. Прикладной шлюз.
29. Виртуальная сеть VPN. Средства обеспечения безопасности.
30. Анализ защищённости и обнаружение атак. Концепция адаптивного управления.
31. Средства анализа защищённости ОС.
32. Классификация систем обнаружения атак IDS.
33. Классификация компьютерных вирусов.

Для оценивания результатов обучения на зачёте (с оценкой) используются следующие показатели:

- Знание сущности и понятие информации, информационной безопасности и характеристику ее составляющих; основных отечественных и зарубежных стандартов в области компьютерной безопасности; основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации; средств и методов предотвращения и обнаружения вторжений; основных методов организационного обеспечения информационной безопасности специальных ИАС; структуры функциональной и обеспечивающих частей специальных ИАС; методов проектирования ИАС.

- Умение применять осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; решать задачи исследования специальных ИАС методами моделирования.

- Владение навыками исследования математических моделей технологических процессов обработки информации в специальных ИАС с целью оценки качества и оптимизации характеристик специальных ИАС; навыками выбора и обоснования критериев эффективности функционирования специальных ИАС; методами применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях; навыками безопасного использования технических средств в профессиональной деятельности.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Глубокие исчерпывающие знания всего программного материала, понимание сущности и взаимосвязи рассматриваемых процессов и явлений. Логически последовательные, полные, правильные и конкретные ответы на все основные вопросы. Правильные и конкретные ответы дополнительные вопросы.	Пороговый уровень и выше порогового	Отлично
Твердые и достаточно полные знания программного материала, понимание сущности рассматриваемых процессов и явлений. Последовательные и правильные, но недостаточно развернутые ответы на основные вопросы. Правильные ответы на дополнительные вопросы.	Пороговый уровень и выше порогового	Хорошо
Правильные и конкретные, без грубых ошибок ответы на основные вопросы. Наличие отдельных неточностей в ответах. В целом правильные ответы с небольшими неточностями на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете, когда количество неправильных ответов превышает количество допустимых для положительной оценки.	Ниже порогового уровня	Неудовлетворительно