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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.С.Шабров
13.05.2022

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.06 Безопасность информационно-аналитических систем

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

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

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра математического анализа

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

7. **Рекомендована:** Научно-методическим Советом математического факультета, Протокол № 0500-03 от 24.03.2022

8. Учебный год: 2025/2026 **Семестр(-ы):** 7

9. Цели и задачи учебной дисциплины:

В результате изучения базовой части цикла обучающийся должен:

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;
- 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 АИС;
- логико-лингвистические основы обработки данных и знаний в специальных АИС;
- методологические основы, методы и средства моделирования предметной области специальных АИС;
- методологические основы, методы и средства моделирования специальных АИС;
- методы построения и исследования математических моделей специальных АИС;
- методы планирования и оптимизации компьютерных экспериментов с моделями специальных АИС;
- методологические основы, методы и средства построения распределенных специальных АИС;
- системы распределенной обработки данных, используемые в специальных АИС;
- нормативную базу, регламентирующую создание и эксплуатацию специальных АИС;
- назначение и классификацию информационных и аналитических систем, систем управления;
- принципы эксплуатации и сопровождения АИС;

уметь:

- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- формализовать предметную область с целью создания баз данных и экспертных систем;
- использовать модели данных и знаний для решения стандартных задач автоматизации;
- решать задачи исследования специальных АИС методами моделирования;
- применять языковые, программные и аппаратные средства исследования эффективности технологических процессов обработки информации в специальных АИС;

- решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных;
- проектировать и сопровождать типовые специальные АИС, локальные сети;
- 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;
- навыками моделирования технологических процессов обработки информации в специальных АИС с заданной степенью статистической надежности результатов;
- навыками исследования математических моделей технологических процессов обработки информации в специальных АИС с целью оценки качества и оптимизации характеристик специальных АИС;
- навыками анализа и синтеза структурных и функциональных схем технологических процессов обработки информации в специальных АИС;
- навыками выбора и обоснования критериев эффективности функционирования специальных АИС;
- навыками анализа программных реализаций;
- 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;
- основами маршрутизации и управления потоками в сетях передачи информации;
- простейшими методами криптографического анализа;
- простейшими методами анализа безопасности криптографических протоколов.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Безопасность информационно-аналитических систем» относится к обязательной части и входит в группу учебных дисциплин "Методы и средства обеспечения информационной безопасности" Федерального государственного образовательного стандарта высшего профессионального образования по направлению 10.05.04 «Информационно-аналитические системы безопасности».

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

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

- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- управление информационной безопасностью.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-6	Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2	Применяет отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	знать: этапы разработки компьютерных моделей систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования, технологии организации и проведения статистического компьютерного моделирования компьютерных систем. уметь: анализировать адекватность модели и результаты модельного эксперимента, сопоставляя получаемые и планируемые результаты. владеть: практическими навыками применения средств и технологий; создания, планирования эксперимента и тестирования компьютерных моделей сложных систем (массового обслуживания, передачи информации, конфликтного взаимодействия систем).
ОПК-11	Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации	ОПК-11.2	Способен разрабатывать систему защиты информации информационно-аналитических систем	знать: базовые понятия информационно-аналитических систем, основы их создания и применения; активные и пассивные методы сбора информации уметь: осуществлять мониторинг информационной безопасности автоматизированных систем, применять системы анализа защищенности владеть: навыками работы с одной из имеющихся на рынке информационно-аналитических систем
ОПК-13	Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла,	ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла	знать: информационные источники и аналитические методы конкурентной разведки, систему мер противодействия промышленному шпионажу, информационные технологии в системе информационно-аналитического обеспечения безопасности

	встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях		информационно-аналитических систем	уметь: использовать организационные, правовые, инженерно-технические и программноаппаратные методы защиты информации владеть: навыками использования информационных, компьютерных и сетевых технологий как средством управления информации

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 4/144.
Форма промежуточной аттестации зачет с оценкой.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)				
	Всего	По семестрам			
		7 сем.			
Аудиторные занятия	64	64			
в том числе: лекции	32	32			
практические					
лабораторные	32	32			
Самостоятельная работа	80	80			
зачет					
Итого:	144	144			

13.1 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
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	Трёхуровневая модель оценки защищённости ИС. Требования к архитектуре ИС. Стандарты. Технологии криптографической защиты информации. Межсетевые

	безопасности.	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	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.
2.2	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.
2.3	Создание архитектуры информационно-аналитических систем (ИАС)	Аналитические системы: процессы и инструменты. Описание общей структуры. Степени ИБ. Особенности применения и анализа информации.

13.2. Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ.	2			5	7
02	Виды угроз ИБ и методы их анализа.	6			15	21
03	Правовое обеспечение ИБ	6			15	21
04	Построение системы ИБ	6		10	15	31
05	Информационные системы (ИС) и обеспечение их безопасности.	6		10	15	31
06	Создание архитектуры информационно-аналитических систем (ИАС)	6		12	15	33
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.

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 зачёту 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 (видеофайлов, файлов-презентаций, файлов с учебными пособиями) по ключевым словам курса и ознакомиться с найденной информацией при подготовке к зачёту по дисциплине.

6. 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, Владимир Александрович**. Информационная безопасность компьютерных систем. Защита целостности информации / В.А. Голуб.– Воронеж: ЛОП ВГУ, 2006.– 31 с.
2	**Смирнов, Сергей Николаевич**. Безопасность систем баз данных / С.Н. Смирнов.– М.: Гелиос АРВ, 2007.– 350 с.
3	**Астанин, Иван Константинович**. Защита информации / И.К. Астанин, Н.И. Астанин.– Воронеж: Воронеж. гос. ун-т, 2006.– с.169
4	**Мельников, Владимир Павлович**. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков.– М.: ACADEMIA, 2006.– 330 с.

б) дополнительная литература:

№ п/п	Источник
5	**Галицкий, Александр Владимирович**. 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	**Завгородний, Виктор Иванович**. Комплексная защита информации в компьютерных системах: Учебное пособие для студ. вузов / В.И. Завгородний.– М.: Логос, 2001.– 262 с.
7	**Гайдамакин, Николай Александрович**. 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, Владимир Васильевич**. Интеллектуальные информационные системы: Компьютерная поддержка систем нечеткой логики и нечеткого вывода / В.В. Круглов, М.И. Дли.– М.: Физматлит, 2002.– 254 с.
8	***Джамбруно, Марк***. Трехмерная графика и анимация / М. Джамбруно.— М.: Вильямс, 2002.— 638 с.
9	***Никулин, Е.А.*** Компьютерная геометрия и алгоритмы машинной графики / Е.А. Никулин.— СПб.: БХВ-Санкт-Петербург, 2003.— 550 с.
10	***Иванова, Т.М.*** Допечатная подготовка. Компьютерная обработка информации / Т.М. Иванова.— СПб.: Питер, 2004.— 366 с.
11	***Панкратова, Татьяна Владимировна***. Обработка цифровых фотографий / Т.В. Панкратова.— СПб.: Питер, 2006.— 271 с.

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

№ п/п	Источник
12	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
13	*Документация по открытому ПО: http://opengl.org.ru, http://inkscape.paint-net.ru, https://inkscape.org/ru/, http://www.gimp.org, http://docs.gimp.org/2.8/ru/*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

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.

Самостоятельная работа студента-бакалавра, 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. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО.

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 7 или 10, Gimp, Inkscape.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Понятия информационной безопасности (ИБ). Ключевые вопросы ИБ.	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Опрос
2	Виды угроз ИБ и методы их анализа.	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Контрольная работа
3	Правовое обеспечение ИБ	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Опрос
4	Построение системы ИБ	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Опрос
5	Информационные системы (ИС) и обеспечение их безопасности.	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Контрольная работа
6	Создание архитектуры информационно-аналитических систем (ИАС)	ОПК -6, ОПК-11, ОПК-13	ОПК-6.2, ОПК-11.2, ОПК-13.4	Опрос
Промежуточная аттестация Форма контроля – зачет с оценкой				КИМ

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Примерный перечень вопросов к зачету

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 криптоключами.
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.

Пример практических заданий

№1. Привести пример действия атакующего и способ защиты от атаки «man-in-the-middle».

№2. Привести пример структуры и функциональности стека протоколов TCP/IP.

Пример контрольно-измерительного материала

1. Анализ угроз информационной безопасности.

2. Международный стандарт ISO 15408.
3. Привести пример структуры и функциональности стека протоколов TCP/IP.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;	Пороговый уровень и/или выше порогового	Зачтено
Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете	Ниже порогового уровня	Незачтено