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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев

(подпись)

30.06.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.54 Управление информационной безопасностью
Код и наименование дисциплины в соответствии с Учебным планом

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

2. Профиль подготовки/специализации: Информационная безопасность финансовых и экономических структур

3. Квалификация (степень) выпускника: специалист

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 **№ 0500-04 от 18.06.2020**г.
(наименование рекомендующей структуры, дата, номер протокола)

8. Учебный год: 2024/2025 **Семестр(-ы):** 9

9. Цели и задачи учебной дисциплины:

В результате изучения базовой части цикла обучающийся должен:

знать:
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- принципы построения современных операционных систем и особенности их применения;
- основные виды и угрозы безопасности операционных систем;
- защитные механизмы и средства обеспечения безопасности операционных систем;
- принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов;
- защитные механизмы и средства обеспечения сетевой безопасности;
- средства и методы предотвращения и обнаружения вторжений;
- основные отечественные и зарубежные стандарты в области компьютерной безопасности;
- основные функциональные возможности современных систем управления базами данных;
- методологические основы теории принятия решений, теории измерений, теории прогнозирования и планирования;
- методы оценки эффективности и качества в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации;

уметь:
- использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач;
- разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем;
- 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;
- профессиональной терминологией в области информационной безопасности;
- навыками работы с инструментальными средствами построения систем представления знаний;
- простейшими методами криптографического анализа;
- простейшими методами анализа безопасности криптографических протоколов.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Управление информационной безопасностью» является вариативной дисциплиной профессионального цикла дисциплин Федерального государственного образовательного стандарта высшего профессионального

образования (ФГОС ВО) по направлению 09.03.05 «Информационно-аналитические системы безопасности».

Дисциплина «Управление информационной безопасностью» базируется на знаниях, полученных по дискретной математике, информатике и безопасности информационных и аналитических систем.

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

выпускник должен обладать следующими компетенциями:

а) общекультурные (ОК):

- способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (**ОК-3**);

- способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (**ОК-5**);

- способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (**ОК-6**);

- способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (**ОК-10**);

б) общепрофессиональные (ОПК):

- способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (**ПК-4**);

- способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (**ПК-5**);

- способностью применять основные защитные механизмы и средства обеспечения безопасности операционных систем (**ПК-8**);

- способностью применять методы защиты информации в информационных и аналитических системах (**ПК-9**);

- способностью учитывать современные тенденции развития прикладной математики и информатики, вычислительной техники, компьютерных технологий в своей профессиональной деятельности (**ПК-18**);

- способностью применять математические модели и методы для решения поставленных задач, в том числе с использованием информационно-аналитических систем (**ПК-19**);

- способностью составлять аналитические документы по вопросам профессиональной деятельности (**ПК-20**);

- способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам проектирования и исследования информационно-аналитических систем безопасности (**ПК-21**);

- способностью оценивать эффективность разрабатываемых информационно-аналитических систем безопасности (**ПК-29**);

- способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (**ПК-34**);

- способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного распространения (**ПК-38**);

- способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей (**ПК-39**).

12. Структура и содержание учебной дисциплины:

12.1 Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 3/108.

12.2 Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)				
	Всего	По семестрам			
		7 сем.	8 сем.	9 сем.	10 сем.
Аудиторные занятия	72			72	
в том числе: лекции	36			36	
практические					
лабораторные	36			36	

СРС	36			36	
Контроль					
Итого:	108			108	

12.3 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
01	Основные понятия информационной безопасности (ИБ)	Понятие информационной безопасности. Объект защиты информации. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Особенности организационной защиты компьютерных информационных систем и сетей.
02	Угрозы информационной безопасности в информационных системах	Основные определения и критерии классификации угроз. Основные угрозы доступности и целостности. Основные угрозы конфиденциальности. Вредительские программы: классификация.
03	Оценочные стандарты в информационной безопасности	Стандарты управления информационной безопасностью. Роль стандартов ИБ. «Оранжевая книга». Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. Основные положения стандартов BS 7799 и ISO/IEC 17799. Международный стандарт ISO/IEC 27001:2005. Сертификация СУИБ на соответствие ISO 27001.
04	Методика оценки рисков информационной безопасности компании	Этапы создания системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков. Управление рисками. Метод оценки рисков на основе модели угроз и уязвимостей. Качественные методики управления рисками. Табличные методы оценки рисков. Методика анализа рисков Microsoft.
05	Правовые меры обеспечения информационной безопасности	Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Общие положения организационной защиты.

12.4 Междисциплинарные связи с другими дисциплинами:

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы	№ № разделов дисциплины рабочей программы, связанных с указанными дисциплинами
1	Принципы построения, проектирования и эксплуатации автоматизированных информационных систем	3, 4, 5
2	Управление информационной безопасностью	3, 4

12.5 Разделы дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	СРС	Всего
01	Основные понятия информационной безопасности (ИБ)	4			4	8
02	Угрозы информационной безопасности в	8		12	8	28

	информационных системах					
03	Оценочные стандарты в информационной безопасности	10		12	8	30
04	Методика оценки рисков информационной безопасности компании	10		12	8	30
05	Правовые меры обеспечения информационной безопасности	4			8	12
Итого		36		36	36	108

13. Учебно-методическое и информационное обеспечение дисциплины:

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов литературы)

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	**Мельников, Владимир Павлович**. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков.– М.: ACADEMIA, 2006.– 330 с.
3	**Голуб, Владимир Александрович**. Информационная безопасность сотовой связи / В.А. Голуб ; Воронеж. гос. ун-т.– Воронеж: ЛОП ВГУ, 2006.– 43 с.

б) дополнительная литература:

№ п/п	Источник
4	**Чмора, Андрей Львович**. Современная прикладная криптография / А.Л.Чмора.– М.: Гелиос АРВ, 2001.– 244 с.
5	**Краковский, Ю.М.** Информационная безопасность и защита информации / Ю.М. Краковский.– М.: Ростов н/Д: МарТ, 2008.– 287 с.
6	**Мао, Венбо**. Современная криптография: теория и практика / Венбо Мао; пер. с англ. и ред. Д.А. Клюшина.– М. [и др.]: Вильямс, 2005.– 763 с.
7	**Безбогов, Александр Александрович**. Безопасность операционных систем / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов.– М.: Гелеос АРВ, 2008.– 319 с.
8	**Завгородний, Виктор Иванович**. Комплексная защита информации в компьютерных системах: Учебное пособие для студ. вузов / В.И. Завгородний.– М.: Логос, 2001.– 262 с.

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

№ п/п	Источник
9	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
10	*Поисковые системы www.google.ru www.yandex.ru*

14. Материально-техническое обеспечение дисциплины:

Учебные аудитории для проведения лекционных и лабораторных занятий. Компьютерные классы для выполнения индивидуальных заданий, оснащённые лицензионным и свободно распространяемым программным обеспечением.

15. Методические рекомендации по организации изучения 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 экзамену 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.

16. Критерии оценки видов аттестации по итогам освоения дисциплины:

В результате освоения дисциплины обучающийся должен:

- Знать: 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; защитные механизмы и средства обеспечения безопасности операционных систем; принципы построения и основные виды симметричных и асимметричных криптографических алгоритмов.
- Уметь: проводить обследование подразделений в целях определения их информационных потребностей; использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; 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; профессиональной терминологией в области информационной безопасности; простейшими методами криптографического анализа; простейшими методами анализа безопасности криптографических протоколов.

16.1 Критерии оценок при сдаче экзамена

16.2 Критерии оценок при сдаче зачета

Зачтено. Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;

Незачтено. Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете.