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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
_____А.Д. Баев
30.05.2019г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.54 Управление информационной безопасностью

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

2. Профиль подготовки/специализация: 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 от № 0500-05 от 27.05.2019 г.

8. Учебный год: 2023/2024 **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» относится к учебным дисциплинам базовой части блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

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

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

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-13	способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их информационной безопасности	знать: - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; - защитные механизмы и средства обеспечения безопасности операционных систем; - 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 владеть: - навыками безопасного использования технических средств в профессиональной деятельности; простейшими методами криптографического анализа; - простейшими методами анализа безопасности криптографических протоколов
ПК-15	способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их	знать: - 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

	работоспособность при внештатных ситуациях	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 уметь: - 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

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

Форма промежуточной аттестации зачёт.

13. 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	

13.1 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
Лекции		
1.1	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.
1.2	Угрозы информационной безопасности в информационных системах	Основные определения и критерии классификации угроз. Основные угрозы доступности и целостности. Основные угрозы конфиденциальности. Вредительские программы: классификация.
1.3	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.
1.4	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.
1.5	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.
Лабораторные работы		
2.1	Анализ рисков на основе программного комплекса	Создание и анализ модели по оценке структуры по заданным стандартам. Оценка уровня обеспечения ИБ организации в соответствии с требованиями СТО. Меры защиты и их характеристики. Формирование отчёта по расчёту рисков. Установление логических связей между возможными рисками и контрмерами.

2.2	Анализ и управление рисками информационной системы	Анализ модели информационных потоков. Понятия: ресурс, сетевая группа, отдел, процессы, пользователи, средства защиты пользователей, информация, средства защиты ресурса и их эффективность, риски и контрмеры (их эффективность). Политики безопасности. Описание отчёта вероятности реализации рисков. Оценка ущерба по видам угроз.
2.3	Анализ рисков на основе модели угроз и уязвимостей	Модель анализа угроз и уязвимостей. Базовые угрозы информационной безопасности. Ресурс, угроза, уязвимость. Категории угроз. Связь ресурс-угроза. Критичность реализации угрозы. Управление рисками и контрмеры.

13.2. Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	СРС	Всего
01	Основные понятия информационной безопасности (ИБ)	6		4	8	18
02	Угрозы информационной безопасности в информационных системах	10		10	8	28
03	Оценочные стандарты в информационной безопасности	6		10	8	24
04	Методика оценки рисков информационной безопасности компании	10		10	10	30
05	Правовые меры обеспечения информационной безопасности	4		2	2	8
Итого		36		36	36	108

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 экзамену 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	*Основы управления информационной безопасностью / А.П. Курило [и др.].– 2-е изд., испр. – Москва: Горячая линия-Телеком, 2014 .– 243 с.*

б) дополнительная литература:

№ п/п	Источник
2	***Мельников, В. П****. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков.– М.: ACADEMIA, 2006.– 330 с.*
3	***Голуб, В. А****. Информационная безопасность сотовой связи / В.А. Голуб ; Воронеж. гос. ун-т.– Воронеж: ЛОП ВГУ, 2006.– 43 с.*
4	***Крапивенский, А. С****. Управление информационной безопасностью в коммерческой рекламной коммуникации / А.С. Крапивенский ; Волгогр. акад. гос. службы; науч. рук. О.В. Байдалова .— Волгоград, 2009 .— 23 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, А. А****. Безопасность операционных систем / А.А. Безбогов, А.В. Яковлев, Ю.Ф. Мартемьянов.– М.: Гелеос АРВ, 2008.– 319 с.*
8	***Завгородний, В. И****. 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	*Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)*

11	*Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)*
12	*Электронно-библиотечная система "РУКОНТ". – (https://rucont.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, 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.

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, MS SQL, Риск-Менеджер.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

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)	ФОС
ПК-13:способность оценивать эффективность специальных ИАС, в том числе средств обеспечения их	знать: - источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения	01, Основные понятия информационной безопасности (ИБ); 03, Оценочные стандарты в информационной	Устный опрос

информационной безопасности	информационной безопасности, принципы построения систем защиты информации; - защитные механизмы и средства обеспечения безопасности операционных систем; - 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	безопасности; 04, Методика оценки рисков информационной безопасности компании	
	уметь: - использовать современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении практических задач; - разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем	02, Угрозы информационной безопасности в информационных системах; 03, Оценочные стандарты в информационной безопасности; 04, Методика оценки рисков информационной безопасности компании	Устный опрос
	владеть: - навыками безопасного использования технических средств в профессиональной деятельности; простейшими методами криптографического анализа; - простейшими методами анализа безопасности криптографических протоколов	03, Оценочные стандарты в информационной безопасности	Практическое задание
ПК-15:способность эксплуатировать	знать: - принципы построения	03, Оценочные стандарты в	Устный опрос,

специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	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	информационной безопасности; 04, Методика оценки рисков информационной безопасности компании; 05, Правовые меры обеспечения информационной безопасности	Контрольное задание
	уметь: - применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	04, Методика оценки рисков информационной безопасности компании	Устный опрос
	владеть: - навыками безопасного использования технических средств в профессиональной деятельности; - профессиональной терминологией в области	03, Оценочные стандарты в информационной безопасности; 04, Методика оценки рисков информационной безопасности	Практическое задание

	информационной безопасности; - навыками работы с инструментальными средствами построения систем представления знаний	компании	

19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации)

Для оценивания результатов обучения на зачёте используются следующие показатели:

- Знание основных понятий информационной безопасности и объектов защиты информации; ключевых составляющих информационной безопасности; особенности организационной защиты компьютерных информационных систем и сетей; критериев классификации угроз; стандартов управления информационной безопасностью и их роли.

- Умение классифицировать возможные виды угроз; создавать поэтапно системы управления ИБ; оценивать защищенность информационной системы компании; оценивать информационные риски на основе модели угроз и уязвимостей и управлять ими.

- Владение основными понятиями информационной безопасности; организации защиты компьютерных информационных систем и сетей; управлением рисками и использовать контрмеры; методами оценки защищенности информационных систем информационных рисков.

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

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень заданий проверки практических навыков

1. Представить схему по управлению информационной безопасностью согласно соглашения об «Уровне Сервиса» (SLA) включая требования по безопасности, а так же соответствующую схему-раздела безопасности SLA, основанную на основе анализа риска.

2. На основе заданной модели с фиксированным уровнем обеспечения ИБ определить требования по мерам её защиты (перечень мер приведён в таблице).
3. По заданной модели информационных потоков установить логические связи между её элементами.
4. По заданной модели анализа угроз и уязвимостей определить уязвимость конкретного ресурса с ценной информацией и слабые места в системе, на основе чего сделать оценку ущерба, который может быть нанесён.
5. Построить по заданной модели ИС перечень контрмер, определив все угрозы на ресурс.
6. Обосновать способы для снижения рисков реализации угрозы по заданным параметрам модели ИС.
7. Проанализировать предложенную к рассмотрению ИС на предмет соответствия требованиям стандарта ISO 17799.
8. Установите контрмеры для невыполненных требований, пороговое значение которых больше 50% (на основе предложенной модели).

Примерный перечень вопросов к зачёту

1. Объект защиты информации.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Критерии классификации угроз.
5. Основные угрозы доступности.
6. Основные угрозы целостности.
7. Основные угрозы конфиденциальности.
8. Вредоносные программы.
9. «Оранжевая книга» как оценочный стандарт.
10. Международный стандарт ISO/IEC 15408.
11. Критерии оценки безопасности информационных систем.
12. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.
13. Международный стандарт ISO/IEC 27001:2005.
14. Системы управления информационной безопасности (СУИБ).
15. Этапы создания системы управления ИБ.
16. Оценка защищенности информационной системы.
17. Оценка информационных рисков.
18. Управление рисками Основные понятия.
19. Метод оценки рисков на основе модели угроз и уязвимостей.
20. Метод оценки рисков на основе модели информационных потоков.
21. Описание архитектуры ИС.
22. Расчет рисков по угрозе конфиденциальность.
23. Качественные методики управления рисками.
24. Количественные методики управления рисками.
25. Табличные методы оценки рисков.
26. Законодательно-правовая база обеспечения информационной безопасности.
27. Идентификация и аутентификация.
28. Управление доступом.
29. Протоколирование и аудит.
30. Контроль целостности.
31. Цифровые сертификаты.

32. Общая политика России в сфере информационной безопасности.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме письменно-устного опроса (индивидуального).

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и защиту контрольной работы, позволяющую оценить степень сформированности умений и навыков.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.