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

УТВЕРЖДАЮ
Заведующий кафедрой
математического моделирования


М.Ш. Бурлуцкая

26.06.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.15 Системы защиты информации от несанкционированного доступа и воздействия

1. Код и наименование специальности:

10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра математического моделирования

6. Составитель программы: Костин Алексей Владимирович к.ф.-м.н.

7. Рекомендована: Научно-методическим советом математического факультета, протокол № 0500-03 от 24.03.2022

8. Учебный год: 2026/2027 **Семестр:** А (10)

9. **Цели и задачи учебной дисциплины**

Цели освоения учебной дисциплины:

- изучить основные угрозы информационной безопасности, их классификацию, причины и виды утечки информации;
- изучить информационные и технические каналы утечки информации.

Задачи учебной дисциплины:

- научиться блокировать и ликвидировать основные угрозы информационным системам;
- научиться создавать и администрировать программное обеспечение, обеспечивающие безопасность информационных систем.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Системы защиты информации от несанкционированного доступа и воздействия» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули).

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен обеспечивать функционирование средств защиты информации в информационно-аналитических системах	ПК-1.2	Способен администрировать системы защиты информации от несанкционированного доступа и воздействия	Знать; как обеспечивать функционирование средств защиты информации в информационно-аналитических системах; Уметь: администрировать системы защиты информации от несанкционированного доступа и воздействия; Владеть: возможностями администрирования систем защиты информации от несанкционированного доступа и воздействия.

12. Объем дисциплины в зачетных единицах/час. — 3/108.

Форма промежуточной аттестации: зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			Семестр А (10)	
Контактная работа		64	64	
в том числе:	лекции	32	32	
	практические	0	0	
	лабораторные	32	32	
	курсовая работа			
	контрольные работы			
Самостоятельная работа		44	44	

Промежуточная аттестация			
Итого:	**108**	**108**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1	Угрозы информационной безопасности	1. Анализ уязвимостей системы. 2. Классификация угроз информационной безопасности. 3. Основные направления и методы реализации угроз.	X
1.2	Построение систем защиты от угрозы нарушения конфиденциальности информации	1. Неформальная модель нарушителя. 2. Методы оценки уязвимости системы. 3. Причины и виды утечки информации.	X
1.3	Защита информации от утечки по техническим каналам	1. Классификация каналов утечки информации. 2. Технические каналы утечки информации. 3. Информационные каналы утечки информации.	X
3. Лабораторные занятия			
3.1	Угрозы информационной безопасности	1. Анализ уязвимостей системы. 2. Классификация угроз информационной безопасности. 3. Основные направления и методы реализации угроз.	X
3.2	Построение систем защиты от угрозы нарушения конфиденциальности информации	1. Неформальная модель нарушителя. 2. Методы оценки уязвимости системы. 3. Причины и виды утечки информации.	X
3.3.	Защита информации от утечки по техническим каналам	1. Классификация каналов утечки информации. 2. Технические каналы утечки информации. 3. Информационные каналы утечки информации.	X

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Угрозы информационной безопасности	8	-	8	20	36
2	Построение систем защиты от угрозы нарушения конфиденциальности информации	12	-	12	12	36
3	Защита информации от утечки по техническим каналам	12	-	12	12	36
	Итого:	32		32	44	108

14. Методические указания для обучающихся по освоению дисциплины:

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций и лабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность, на которую отводится 44 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Системы защиты информации от несанкционированного доступа и воздействия» предполагает выполнение следующих заданий:

1) самостоятельное изучение учебных материалов по разделам дисциплины с использованием основной и дополнительной литературы, информационно-справочных и поисковых систем;

2) подготовку к текущим аттестациям: выполнение лабораторных заданий по поиску необходимых для работы в аудитории материалов в Интернете.

Особое внимание обучающихся направляется на изучение возможных типов угроз информационной безопасности, построению систем защиты от угрозы нарушения конфиденциальности информации, защите информации от утечки по техническим каналам.

Все выполняемые студентами самостоятельно задания подлежат последующей проверке преподавателем для получения допуска к зачету.

В случае необходимости перехода на дистанционный режим обучения будет создан электронный курс на портале «Электронный университет ВГУ»: edu.vsu.ru. Там же будут размещены необходимые для усвоения курса материалы.

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

а) основная литература:

№ п/п	Источник
1	Краковский Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 .
2	Васильев В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И. Васильев. — 3-е изд., стереотип. — Москва : Машиностроение, 2021. — 172 с. — ISBN 978-5-907104-99-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192986 .

б) дополнительная литература:

№ п/п	Источник
3	Панфилов И. В. Проблемы защиты информации в компьютерных сетях и системах : учебное пособие / И. В. Панфилов, А. М. Заяц, Е. И. Панфилова. — Санкт-Петербург : СПбГЛТУ, 2008. — 148 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/45554 .
4	Петровский В. И. Принципы построения системы защиты информации на предприятиях различных форм собственности : учебное пособие / В. И. Петровский ; под редакцией В. И. Петровского. — Казань : КНИТУ-КАИ, 2016. — 512 с. — ISBN 978-5-7579-2150-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149575 .
5	

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
6	Электронный каталог ЗНБ ВГУ : http://www.lib.vsu.ru .
7	https://math.vsu.ru/wp/?page_id=937 – раздел на сайте математического факультета, на котором размещены методические издания.
8	Доктрина информационной безопасности Российской Федерации

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Краковский Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

	https://e.lanbook.com/book/156401 .: электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401
2	Васильев В. И. Интеллектуальные системы защиты информации : учебное пособие / В. И. Васильев. — 3-е изд., стереотип. — Москва : Машиностроение, 2021. — 172 с. — ISBN 978-5-907104-99-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192986 .
3	Петровский В. И. Принципы построения системы защиты информации на предприятиях различных форм собственности : учебное пособие / В. И. Петровский ; под редакцией В. И. Петровского. — Казань : КНИТУ-КАИ, 2016. — 512 с. — ISBN 978-5-7579-2150-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/149575 .
4	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете.

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

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ» (https://edu.vsu.ru).

Перечень необходимого программного обеспечения: Win10pro или Linux, Microsoft Office, LibreOffice 6, Calc, Microsoft Visual Studio, Microsoft Visual C++, Foxit Reader, браузер Mozilla Firefox, Opera или Internet.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации со специализированной мебелью.

Для самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Угрозы информационной безопасности	ПК-1	ПК-1.2	Комплект лабораторных заданий № 1, 2, 3
2.	Построение систем защиты от угрозы нарушения конфиденциальности информации	ПК-1	ПК-1.2	Комплект лабораторных заданий № 4, 5, 6
3.	Защита информации от утечки по техническим каналам	ПК-1	ПК-1.2	Комплект лабораторных заданий № 7, 8, 9
Промежуточная аттестация Форма контроля – зачет				Перечень вопросов к зачету

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: устных опросов, проверки домашних заданий, лабораторных работ,

Перечень лабораторных работ:

1. Анализ уязвимостей системы.
2. Классификация угроз информационной безопасности.
3. Основные направления и методы реализации угроз.
4. Неформальная модель нарушителя.
5. Методы оценки уязвимости системы.
6. Причины и виды утечки информации.
7. Классификация каналов утечки информации.
8. Технические каналы утечки информации.
9. Информационные каналы утечки информации.

Для оценивания текущего контроля успеваемости используются следующие ***показатели:***

1. знание основных понятий и методов;
2. умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений;
3. владение математическим аппаратом и современными методами в теории защиты информации;
4. умение писать код компьютерных программ для решения типовых математических задач;
5. знание имеющихся ресурсов для решения прикладных математических задач;
6. умение использовать стандартные пакеты программного обеспечения для решения типовых математических задач;
7. владение навыками хранения, поиска, сбора, систематизации, обработки и использования информации.

Шкала оценок:

Зачтено: Выполнение заданий соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.

Не зачтено: Ответы не соответствуют ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется в форме собеседования по результатам выполнения лабораторных работ.

Перечень вопросов к зачету:

1. Анализ уязвимостей системы.
2. Классификация угроз информационной безопасности.
3. Основные направления и методы реализации угроз.
4. Неформальная модель нарушителя.
5. Методы оценки уязвимости системы.
6. Причины и виды утечки информации.
7. Классификация каналов утечки информации.
8. Технические каналы утечки информации.
9. Информационные каналы утечки информации.

Для оценивания результатов обучения на зачете используются следующие **показатели:**

1) знание теоретических основ;
2) умение решать задачи;
3) умение работать с алгоритмами методов и информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатов используется шкала: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения показаны в следующей таблице:

Критерии оценивания	Шкала оценок
Ответ соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.	«Зачтено»
Ответ не соответствует ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие.	«Не зачтено»