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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
Шабров С.А.

17.04.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.13 Информационная безопасность

1. Код и наименование направления подготовки/специальности: 02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: Математическое и компьютерное моделирование

3. Квалификация выпускника: бакалавр

4. Форма обучения: очная

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

6. Составители программы: Шабров Сергей Александрович, доктор физико-математических наук, доцент

7. Рекомендована: Научно-методическим Советом математического факультета,

протокол от 28.03.2024 №0500-03

8. Учебный год: 2027-2028 **Семестр(ы): 8**

9. **Цели и задачи учебной дисциплины**

Цели освоения учебной дисциплины:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи учебной дисциплины:

- изучение характеристик основных угроз информационной безопасности, каналов утечки информации и методов компьютерного шпионажа;
- получение представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от модификации и удаления;
- освоение критериев эффективности мер по защите информации.

10. Место учебной дисциплины в структуре ООП:

учебная дисциплина Информационная безопасность относится к обязательной части Блока 1.

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-2	Способен использовать современные информационные технологии при решении задач математического и компьютерного моделирования	ПК-2.1	Способен строить алгоритмы и реализовывать их программными методами, в том числе на базе пакетов прикладных программ	Знать: принципы проектирования и разработки программных продуктов, критерии их качества Уметь: оценить качество программ и пакетов прикладных программ Владеть: навыками реализации программных продуктов
		ПК-2.2	Способен использовать современные методы математического и компьютерного моделирования при решении теоретических и прикладных задач	Знать: методы формализации задачи на основе математического моделирования и теории приближенных методов Уметь: свести поставленную задачу к этапам алгоритмизации и программирования Владеть: навыками формализации и подбора метода решения

12. Объем дисциплины в зачетных единицах/час. — 2 / 72.

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		8	№ семестра	…

Аудиторные занятия					
в том числе:	лекции	12	12		
	практические				
	лабораторные	12	12		
Самостоятельная работа		48	48		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*					
Итого:		72	72		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1.	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.	
1.2.	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	
1.3.	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы	

		каналов несанкционированного получения информации. Причины нарушения целостности информации.	
1.4.	Теоретические основы методов защиты информационных систем	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.	
1.5.	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.	
2. Практические занятия			
2.1			
2.2			
3. Лабораторные занятия			
3.1	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.	
3.2	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны.	

		Концепция информационной безопасности.	
3.3	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.	
3.4	Теоретические основы методов защиты информационных систем	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.	
3.5	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.	

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	Общие вопросы информационной безопасности	2		2	8	12
2	Государственная система информационной безопасности	2		2	8	12
3	Угрозы безопасности	2		2	8	12
4	Теоретические основы методов защиты информационных систем	2		2	12	16
5	Методы защиты средств вычислительной техники	4		4	12	20
	Итого:	12		12	48	72

14. Методические указания для обучающихся по освоению дисциплины: *(рекомендации обучающимся по освоению дисциплины: указание наиболее сложных разделов, работа с*

конспектами лекций, презентационным материалом, рекомендации по выполнению курсовой работы, по организации самостоятельной работы по дисциплине и др.)

Для обеспечения систематической и регулярной работы по изучению дисциплины и успешного прохождения аттестаций студентам рекомендуется придерживаться следующего порядка обучения:
Самостоятельно определить объем времени, необходимого для проработки каждой темы.
Регулярно изучать каждую тему дисциплины как по конспектам лекции, так и по рекомендованной литературе, используя различные формы индивидуальной работы.
Согласовывать с преподавателем виды работы по изучению дисциплины
По завершении отдельных тем передавать выполненные работы (домашние задания) преподавателю.
При успешном прохождении рубежных контрольных испытаний студент может претендовать на сокращение программы промежуточной (итоговой) аттестации по дисциплине.

Методические указания для обучающихся при самостоятельной работе.

1 Самостоятельная работа обучающихся направлена на самостоятельное освоение всех тем и вопросов учебной дисциплины, предусмотренных программой. Самостоятельная работа является обязательным видом деятельности для каждого обучающегося, ее объем по учебному курсу определяется учебным планом. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.
2 Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся заинтересованное отношение к конкретной проблеме.
3 Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.
4 Для успешного и плодотворного обеспечения итогов самостоятельной работы разработаны учебно-методические указания к самостоятельной работе студентов над различными разделами дисциплины.
5 Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий (практических и теоретических); выполнение контрольных работ; подготовка к практическим занятиям; работа с вопросами для самопроверки.
6 Все задания, выполняемые студентами самостоятельно, подлежат последующей проверке преподавателем.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Голуб, Владимир Александрович. Информационная безопасность СМИ: криптографическая защита информации : учебное пособие / В.А. Голуб ; Воронеж. гос. ун-т, Фак. журналистики .— Воронеж : Факультет журналистики ВГУ, 2010 .— 99 с.*

б) дополнительная литература:

№ п/п	Источник
1	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
2	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.
3	Мещеряков Р. В., Шелупанов А. А., Белов Е. Б., Лось В. П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
4	Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994.
5	Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: «Инкомбук», 1997. – 540 с.

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

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)
2	ЭБС «Университетская библиотека онлайн»
3	http://www.math.vsu.ru – официальный сайт математического факультета ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных), курсовых работ и др.)*

№ п/п	Источник
1	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
2	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информаци-онной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.

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

Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации. Лабораторные занятия ведутся с привлечением мультимедийных технологий.

Microsoft Windows 10, Foxit Reader, 7-Zip, Mozilla Firefox

---

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных и лабораторных занятий используются аудитории и компьютерные лаборатории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для самостоятельной работы используются классы с компьютерной техникой, оснащенные 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.	Общие вопросы информационной безопасности	ПК-2	ПК – 2.1, ПК – 2.2	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
2.	Государственная система информационной безопасности	ПК-2	ПК – 2.1, ПК – 2.2	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
	Угрозы безопасности	ПК-2	ПК – 2.1, ПК – 2.2	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
	Теоретические основы методов защиты информационных систем	ПК-2	ПК – 2.1, ПК – 2.2	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
	Методы защиты средств вычислительной техники	ПК-2	ПК – 2.1, ПК – 2.2	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
Промежуточная аттестация форма контроля – экзамен				Вопросы к экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

письменная работа (два вопроса):

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
19. Биометрические средства идентификации и аутентификации пользователей.
20. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
21. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
23. Законодательный уровень применения цифровой подписи.
24. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
26. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
27. Средства обеспечения информационной безопасности в ОС Windows’2000. Разграничение доступа к данным. Групповая политика.
28. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
29. Применение средств Windows для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
30. Разграничение доступа к данным в ОС семейства UNIX.
31. Пользователи и группы в ОС UNIX.
32. Пользователи и группы в ОС Windows.
33. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
34. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
35. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
36. Распределенные информационные системы. Удаленные атаки на информационную систему.
37. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.

38. Физические средства обеспечения информационной безопасности.
39. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
40. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
41. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
42. Виртуальные частные сети, их функции и назначение.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

контрольно-измерительные материалы к зачету:

1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена.
4. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации.
5. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
7. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности.
8. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации.
9. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
10. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
11. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.
12. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
13. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.
14. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы.
15. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
16. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы.
17. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

1. Создание политики информационной безопасности должно учитывать следующие основное число направлений защиты:

1) четыре
2) пять
3) шесть
4) семь

2. При разработке и реализации политики ИБ целесообразно руководствоваться следующим количеством принципов:

1) 6
2) 8
3) 9
4) 10

3. Обязательным условием начала разработки политики ИБ является:

1) наличие на фирме службы защиты информации
2) наличие на фирме функционирующей ИС
3) наличие на фирме высококвалифицированных специалистов в области защиты информации
4) возможность привлечения к разработке политики ИБ сторонних специалистов

4. В политике ИБ должны содержаться следующее число групп сведений:

1) три
2) четыре
3) пять
4) шесть

5. В число основных видов защищаемых ресурсов ИС входит:

1) данные
2) инфраструктура
3) аппаратные средства
4) программное обеспечение

6. Безопасность предприятия включает следующее число компонент:

1) два
2) четыре
3) шесть
4) восемь

7. Преимуществом мандатного метода управления доступом, используемого в в соответствующей политике ИБ, является:

1) обеспечение более высокой надежности работы самой ИС
2) простота определения правил разграничения доступа
3) широкое распространение данного метода для работы с конфиденциальной информацией
4) предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности

8. Основные положения политики безопасности организации описываются в следующих документах:

1) обзор политики безопасности
2) обзор защищаемой инфраструктуры предприятия
3) описание базовой политики безопасности
4) руководство по архитектуре безопасности

9. Основные положения политики безопасности организации описываются в следующем количестве документов:

1) три
2) четыре
3) пять
4) шесть

10. План, определяющий границы системы, для которой разрабатывается политика ИБ, включает следующее число пунктов:

1) три
2) четыре
3) пять
4) шесть

11. Понятие «безопасность предприятия » для любой организации включает в себя:

1) физическую безопасность
2) информационную безопасность
3) безопасность взаимосвязанных объектов предприятия
4) экономическую безопасность

12. Варианты реализации стратегии управления рисками включают следующее их число:

1) два
2) три
3) четыре
4) пять

13. В описании базовой политики безопасности определяются:

1) разрешенные действия
2) запрещенные действия
3) все вышеуказанные действия+
4) средства управления в рамках реализуемой архитектуры безопасности

14. Специализированные политики безопасности подразделяются на следующее число групп:

1) две
2) три
3) четыре
4) пять

15. К специализированным политикам, затрагивающим значительное число пользователей, относятся:

1) политика защиты информации
2) политика удаленного доступа к ресурсам сети;
3) политика безопасности виртуальных защищенных сетей
4) политика допустимого использования

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.