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

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.07 Безопасность программного обеспечения

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

2. Профиль подготовки/специализация: "Автоматизация информационно-аналитической деятельности", "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 **№0500-07 ОТ 29.06.2021**.

8. Учебный год: 2024/2025 **Семестр: 9**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:
- знание принципов построения современных операционных систем и особенности их применения;
- знание основных видов и угроз безопасности операционных систем;
- знание защитных механизмов и средства обеспечения безопасности операционных систем;
- знание средств и методов хранения и передачи информации;
- знание защитных механизмов и средств обеспечения сетевой безопасности;
- знание средств и методов предотвращения и обнаружения вторжений;
- уметь применять средства антивирусной защиты и обнаружения вторжений;

Задачи учебной дисциплины:
- умение осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- применять навыки безопасного использования технических средств в профессиональной деятельности;
- владение профессиональной терминологией в области информационной безопасности;
- владение навыками настройки межсетевых экранов;
- владение методикой анализа сетевого трафика;
- владение методикой анализа результатов работы средств обнаружения вторжений.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Безопасность программного обеспечения» относится к учебным дисциплинам обязательной части блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

Дисциплина «Безопасность программного обеспечения» базируется на знаниях, полученных по дискретной математике, информатике, математической логике и теории алгоритмов, безопасности сетей ЭВМ.

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

- современные платежные системы и их безопасность.

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

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-11.3	Осуществляет меры противодействия нарушениям безопасности с	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих;

	использованием различных программных и аппаратных средств защиты	- источники и классификацию угроз информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; средства и методы хранения и передачи информации; - математические модели шифров; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - применять средства антивирусной защиты и обнаружения вторжений владеть: - методикой анализа сетевого трафика; - методикой анализа результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности компьютерным системам
ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	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; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности уметь: - применять средства антивирусной защиты и обнаружения вторжений; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - пользоваться средствами защиты, предоставляемыми системами управления базами данных владеть:

		- навыками безопасного использования технических средств в профессиональной деятельности; - навыками настройки межсетевых экранов; - методикой анализа результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности компьютерным системам

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

Форма промежуточной аттестации зачёт.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра: 9	№ семестра	…
Аудиторные занятия		32	32		
в том числе:	лекции	18	18		
	практические				
	лабораторные	18	18		
Самостоятельная работа		36	36		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачёт)*					
Итого:		72	72		

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
Лекции			
1.1	Введение в теорию обеспечения безопасности программного обеспечения	Основные причины защиты программного обеспечения (ПО). Классификация угроз безопасности ПО. Примеры реализации угроз безопасности ПО в современном мире. Основная аксиоматика и терминология. Жизненный цикл ПО компьютерных систем. Моделирование угроз	–

		безопасности ПО. Основные принципы обеспечения безопасности ПО.	
1.2	Технологическая сторона осуществления безопасности ПО	Методы доказательства "правильных" программ и их спецификаций. Средства и методы анализа безопасности ПО. Моделирование контроля обеспечения надёжности технологической безопасности ПО. Алгоритмы создания безопасных процедур. Классификация подходов к защите разрабатываемых программ. Методы идентификации программ и их характеристик.	–
1.3	Эксплуатационная сторона осуществления безопасности ПО	Методы и средства защиты ПО от компьютерных вирусов. Внедрение методов защиты ПО на этапе его эксплуатации. Классификация средств проверки целостности и достоверности программного кода ПО. Основные подходы к защите ПО от несанкционированного копирования.	–
1.4	Правовая сторона организации разработки программ по обеспечению безопасности	Нормативные документы, регламентирующие защищённость ПО. Стандарты. Сертификационные испытания ПО. Психология программирования. Человеческий фактор.	–
Лабораторные работы			
2.1	Безопасная эксплуатация web-браузеров	Приобретение навыков безопасной работы в сети Интернет, создание безопасной конфигурации web-браузеров, анализа и контроля механизма cookies.	–
2.2	Контроль и управление доступом в операционных системах	Освоение средств контроля и управления доступом пользователей к ресурсам операционной системы, приобретение навыков распределения прав на примере	–

		файловой системы NTFS в среде Windows.	
2.3	Анализ программных потайных ходов и защита от них	Анализ структуры, функциональности и угроз программных потайных ходов, а также изучение методов защиты от них.	–
2.4	Методы надёжной передачи данных	Освоение метода Хемминга помехоустойчивого кодирования, позволяющего обнаруживать и автоматически исправлять ошибки, возникающие при хранении и передаче информации.	–
2.5	Защита программного обеспечения от несанкционированного доступа	Получение практических навыков защиты программного обеспечения от несанкционированного доступа с помощью паролей.	–
2.6	Защита программ от нелегального использования	Приобретение навыков защиты приложений от нелегального использования, анализа исполняемых кодов в отсутствии исходных текстов и применения способов защиты программ от дизассемблирования и отладки.	–

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Введение в теорию обеспечения безопасности программного обеспечения	4		4	10	18
02	Технологическая сторона осуществления безопасности ПО	6		4	8	18
03	Эксплуатационная сторона осуществления безопасности ПО	6		8	14	28
04	Правовая сторона организации разработки программ по обеспечению безопасности	2		2	4	8
Итого		18		18	36	72

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 по ключевым словам курса (видеофайлов, файлов-презентаций, файлов с учебными пособиями) и ознакомиться с найденной информацией при подготовке к зачёту 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	*Программно-аппаратные средства обеспечения информационной безопасности / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов; под редакцией А.В. Душкина. – Москва: Горячая линия-Телеком, 2018. – 248 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111053*
2	***Алешкин, А.С.*** *Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) / А.С. Алешкин, С.А. Лесько, Д.О. Жуков. – Москва: РТУ МИРЭА, 2020. – 152 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/167600*
3	*Конспект лекций по курсу Математические основы защиты информации и информационной безопасности / Б.Н. Воронков, Ю.А. Крыжановская. – Воронеж: ВГУ, 2017. – 77 с. – [Электронный ресурс] // URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m17-76.pdf*
4	***Голуб, В.А.*** *Информационная безопасность СМИ: криптографическая защита информации / В.А. Голуб . – Воронеж: Факультет журналистики ВГУ, 2010. – 99 с.*

б) дополнительная литература:

№ п/п	Источник
5	***Казарин, О.В.*** *Безопасность программного обеспечения компьютерных*

	систем [Электронный ресурс]. – М.: МГУЛ, 2003. – 212 с. – режим доступа http://window.edu.ru/resource/846/23846/files/kazarin.pdf, свободный.
6	***Краковский, Ю.М.** Информационная безопасность и защита информации / Ю.М. Краковский.– М.: Ростов н/Д: МарТ, 2008.– 287 с.*
7	***Галицкий, А. В**. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин.– М.: ДМК Пресс, 2004.– 613 с.*
8	***Бабенко, Л. К**. Защита информации с использованием смарт-карт и электронных брелоков / Л.К. Бабенко, С.С. Ищуков, О.Б. Макаревич.– М.: Гелиос АРВ, 2003.– 351с.*
9	***Черемушкин, А. В**. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин.– М.: Академия, 2009.– 271 с.*
10	***Аграновский, А. В**. Практическая криптография: Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади.– М.: СОЛОН-Пресс, 2002.– 254с.*

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

№ п/п	Источник
11	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
12	*Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)*
13	*Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)*
14	*Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	*Практикум по администрированию программного обеспечения / И.В. Анзин. – Ставрополь: СКФУ, 2017. – 85 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/155248*
2	***Ермакова, А.Ю.** Методы и средства защиты компьютерной информации / А.Ю. Ермакова. – Москва: РТУ МИРЭА, 2020. – 223 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/163844*
3	***Проскурин, В.Г.** Защита в операционных системах / В.Г. Проскурин. – Москва: Горячая линия-Телеком, 2016. – 192 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111091*

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 на платформе образовательного портала «Электронный университет ВГУ».

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

При осуществлении самостоятельной работы возможна интерактивная связь с преподавателем через сеть интернет на платформе образовательного портала «Электронный университет ВГУ». Проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО на системах с ОС: Windows 10 и Ubuntu 20.04.

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 10, Ubuntu 20.04, Linux, специализированное антивирусное ПО DrWeb Enterprise Security Suite, сниффер Wireshark, программное обеспечение для виртуализации персонального компьютера Oracle VM VirtualBox, web-браузер Mozilla Firefox. В ходе лабораторных занятий задействуется учебно-лабораторный стенд «Сетевая безопасность», сертифицированный аппаратно-программный модуль «Соболь».

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

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)	Оценочные средства
ОПК-11.3: Осуществляет меры противодействия нарушениям безопасности с использованием различных программных и	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - источники и классификацию угроз	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления	Устный опрос

аппаратных средств защиты	информационной безопасности; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; средства и методы хранения и передачи информации; - математические модели шифров; - средства и методы предотвращения и обнаружения вторжений; - основные отечественные и зарубежные стандарты в области компьютерной безопасности	безопасности ПО; 04, Правовая сторона организации разработки программ по обеспечению безопасности	
	уметь: - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - применять средства антивирусной защиты и обнаружения вторжений	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	Устный опрос
	владеть: - методикой анализа сетевого трафика; - методикой анализа результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности компьютерным системам	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	Практическое задание
ОПК-13.4: Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-	знать: - принципы построения современных операционных систем и особенности их применения; - основные виды и угрозы безопасности операционных систем;	01, Введение в теорию обеспечения безопасности программного обеспечения; 02, Технологическая сторона	Устный опрос

аналитических систем	- защитные механизмы и средства обеспечения безопасности операционных систем; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности	осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО; 04, Правовая сторона организации разработки программ по обеспечению безопасности	
	уметь: - применять средства антивирусной защиты и обнаружения вторжений; - осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; - пользоваться средствами защиты, предоставляемыми системами управления базами данных	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	Устный опрос
	владеть: - навыками безопасного использования технических средств в профессиональной деятельности; - навыками настройки межсетевых экранов; - методикой анализа результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности компьютерным системам	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	Практическое задание

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:

- Тестовые задания;
- Лабораторные работы;
- Контрольная работа.

Примерный перечень заданий проверки практических навыков

1. Представить доказательство правильности программы, представленной блок-схемой.
2. Сформировать безопасную конфигурацию web-браузеру Mozila.
3. Определить криптоустойчивость заданного пароля.
4. Провести на примере сравнительный анализ оценки информационной сложности программного обеспечения метриками (на выбор) Холстеда, Маккейба, Джилба и Чепина.
5. Сформировать блок шифрования программы для исключения открытого хранения пароля.
6. Провести разграничение доступа к созданной папке.
7. Провести анализ заданного файла cookies.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- Собеседование по билетам к зачету.

Примерный перечень вопросов к зачёту

1. Основные угрозы программного обеспечения (ПО).
2. Жизненный цикл ПО.
3. Технологическая безопасность ПО.
4. Эксплуатационная безопасность ПО.
5. Модель угроз ПО.
6. Принципы обеспечения безопасности ПО.
7. Формальные методы доказательства правильности программ.
8. Спецификации методов доказательства правильности программ.
9. Методы анализа безопасности ПО.
10. Методы обеспечения надёжности программ для контроля их технологической безопасности.
11. Стандарты создания алгоритмически безопасных процедур.
12. Классификация подходов к защите разрабатываемых программ.
13. Методы идентификации программ и их характеристик.
14. Средства защиты программ от компьютерных вирусов.
15. Методы обеспечения целостности используемого программного кода.
16. Средства обеспечения достоверности программного кода.
17. Защита программ от несанкционированного копирования.
18. Нормативные документы, регламентирующие защищённость ПО.
19. Сертификационные испытания программных средств.
20. Человеческий фактор в процессе программирования.

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; применять средства антивирусной защиты и обнаружения вторжений; оценивать информационные риски на основе модели угроз и уязвимостей и управлять ими; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

- 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