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.34 Безопасность программного обеспечения

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: 2022/2023 **Семестр(ы):** 7

9. Цели и задачи учебной дисциплины:

В результате изучения базовой части цикла обучающийся должен:

знать:
- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- 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;
- средства и методы хранения и передачи информации;
- математические модели шифров;
- криптографические стандарты;
- базовые криптографические протоколы и основные требования к ним;
- механизмы реализации атак в компьютерных сетях;
- защитные механизмы и средства обеспечения сетевой безопасности;
- средства и методы предотвращения и обнаружения вторжений;
- основные отечественные и зарубежные стандарты в области компьютерной безопасности;
- требования, методы и средства информационной безопасности в технологиях платежных систем;

уметь:
- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- 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;
- профессиональной терминологией в области информационной безопасности;
- навыками настройки межсетевых экранов;
- методикой анализа сетевого трафика;
- методикой анализа результатов работы средств обнаружения вторжений;
- методами и средствами выявления угроз безопасности компьютерным системам;
- простейшими методами криптографического анализа.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Безопасность программного обеспечения» относится к учебным дисциплинам базовой 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:

- управление информационной безопасностью.

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	
ОПК-7	способность применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; - 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; - требования, методы и средства информационной безопасности в технологиях платежных систем уметь: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - 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; - простейшими методами криптографического анализа
ПК-15	способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	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; - криптографические стандарты; - базовые криптографические протоколы и основные требования к ним; - 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/часах в соответствии с учебным планом — 2/72.

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	32	32			
в том числе: лекции	16	16			
практические					
лабораторные	16	16			
СРС	40	40			
Контроль					
Итого:	72	72			

13.1 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
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 раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	СРС	Всего
01	Введение в теорию обеспечения безопасности программного обеспечения	4		4	12	20
02	Технологическая сторона осуществления безопасности ПО	5		4	8	17
03	Эксплуатационная сторона осуществления безопасности ПО	5		8	14	27
04	Правовая сторона организации разработки программ по обеспечению безопасности	2			6	8
Итого		16		16	40	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 (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	***Ищейнов, В. Я****. Защита конфиденциальной информации / В.Я. Ищейнов, М.В. Мецатунян.– М.: ФОРУМ, 2009.– 254 с.*
2	***Некраха, А. В****. Организация конфиденциального делопроизводства и защита информации / А.В. Некраха, Г.А. Шевцова.– М.: Академический Проект, 2007.– 219 с.*
	Голуб, В.А. *Информационная безопасность СМИ: криптографическая защита информации : / В.А. Голуб . – Воронеж : Факультет журналистики ВГУ, 2010 . – 99 с.*
3	***Астанин, И. К****. Защита информации / И.К. Астанин, Н.И. Астанин.– Воронеж: Воронеж. гос. ун-т, 2006.– с.169*

б) дополнительная литература:

№ п/п	Источник
4	***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.*
5	***Краковский, Ю.М.*** *Информационная безопасность и защита информации / Ю.М. Краковский.– М.: Ростов н/Д: МарТ, 2008.– 287 с.*
6	***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.*
7	***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.*

8	***Черемушкин, А. В**. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин.– М.: Академия, 2009.– 271 с.*
9	***Аграновский, А. В**. Практическая криптография: Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади.– М.: СОЛОН-Пресс, 2002.– 254с.*
10	***Живетин, В. Б**. Риски и безопасность экономических систем (математическое моделирование) / В.Б. Живетин.– М.: Ин-т проблем риска, 2008.– 431 с.*

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:

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: VirtualBox, MS Visual Studio 2010.

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, VirtualBox, MS Visual Studio 2010.

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
ОПК-7:способность применять методы и средства обеспечения информационной безопасности специальных ИАС	знать: - сущность и понятие информации, информационной безопасности и характеристику ее составляющих; 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; - требования, методы и средства информационной безопасности в технологиях платежных систем	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО; 04, Правовая сторона организации разработки программ по обеспечению безопасности	Устный опрос
	уметь: - классифицировать защищаемую информацию по видам	02, Технологическая сторона осуществления	Устный опрос

	тайны и степеням конфиденциальности; - классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; - применять средства антивирусной защиты и обнаружения вторжений	безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	
	владеть: - методикой анализа сетевого трафика; - методикой анализа результатов работы средств обнаружения вторжений; - методами и средствами выявления угроз безопасности компьютерным системам; - простейшими методами криптографического анализа	02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО	Практическое задание
ПК-15:способность эксплуатировать специальные ИАС и средства обеспечения их информационной безопасности на всех этапах жизненного цикла, а также восстанавливать их работоспособность при внештатных ситуациях	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; - криптографические стандарты; - базовые криптографические протоколы и основные требования к ним; - механизмы реализации атак в компьютерных сетях; - защитные механизмы и средства обеспечения сетевой безопасности	01, Введение в теорию обеспечения безопасности программного обеспечения; 02, Технологическая сторона осуществления безопасности ПО; 03, Эксплуатационная сторона осуществления безопасности ПО; 04, Правовая сторона организации разработки программ по обеспечению безопасности	Устный опрос

	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

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 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.

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.

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.