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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа

А.Д. Баев

(подпись)

30.06.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.34 Безопасность программного обеспечения

Код и наименование дисциплины в соответствии с Учебным планом

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

2. Профиль подготовки/специализации: Информационная безопасность финансовых и экономических структур

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

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

6. Составители программы:
Найдюк Филипп Олегович, канд. физ.-мат. наук, доцент кафедры математического анализа

7. **Рекомендована:** Научно-методическим Советом математического факультета протокол **№ 0500-04 от 18.06.2020**г.

(наименование рекомендующей структуры, дата, номер протокола)

8. Учебный год: 2023/2024 **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» является вариативной дисциплиной профессионального цикла дисциплин Федерального государственного образовательного стандарта высшего профессионального образования (ФГОС ВО) по направлению 09.03.05 «Информационно-аналитические системы безопасности».

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

11. Компетенции обучающегося, формируемые в результате освоения дисциплины:

выпускник должен обладать следующими компетенциями:

а) общекультурные (ОК):

- способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (**ОК-3**);

- способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (**ОК-5**);

- способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (**ОК-6**);

- способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности (**ОК-10**);

б) общепрофессиональные (ОПК):

- способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (**ПК-4**);

- способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (**ПК-5**);

- способностью применять основные защитные механизмы и средства обеспечения безопасности операционных систем (**ПК-8**);

- способностью применять методы защиты информации в информационных и аналитических системах (**ПК-9**);

- способностью учитывать современные тенденции развития прикладной математики и информатики, вычислительной техники, компьютерных технологий в своей профессиональной деятельности (**ПК-18**);

- способностью применять математические модели и методы для решения поставленных задач, в том числе с использованием информационно-аналитических систем (**ПК-19**);

- способностью составлять аналитические документы по вопросам профессиональной деятельности (**ПК-20**);

- способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам проектирования и исследования информационно-аналитических систем безопасности (**ПК-21**);

- способностью оценивать эффективность разрабатываемых информационно-аналитических систем безопасности (**ПК-29**);

- способностью организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности (**ПК-34**);

- способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного распространения (**ПК-38**);

- способностью обосновывать решения, связанные с реализацией правовых норм в пределах должностных обязанностей (**ПК-39**).

12. Структура и содержание учебной дисциплины:

12.1 Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 2/72.

12.2 Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)				
	Всего	По семестрам			
		7 сем.	8 сем.	9 сем.	10 сем.
Аудиторные занятия	36			36	
в том числе: лекции	18			18	
практические					
лабораторные	18			18	
СРС	36			36	
Контроль					
Итого:	72			72	

12.3 Содержание разделов дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
01	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.
02	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.
03	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.
04	Правовая сторона организации разработки программ по обеспечению безопасности	Нормативные документы, регламентирующие защищённость ПО. Стандарты. Сертификационные испытания ПО. Психология программирования. Человеческий фактор.

12.4 Междисциплинарные связи с другими дисциплинами:

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы	№ № разделов дисциплины рабочей программы, связанных с указанными дисциплинами
1	Безопасность информационных и аналитических систем	1, 2, 3
2	Управление информационной безопасностью	2, 3

12.5 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	6		12	10	28

02	Технологическая сторона осуществления безопасности ПО	5		6	2	13
03	Эксплуатационная сторона осуществления безопасности ПО	5		16	2	23
04	Правовая сторона организации разработки программ по обеспечению безопасности	2		2	4	8
Итого		18		36	18	72

13. Учебно-методическое и информационное обеспечение дисциплины:

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов литературы)

а) основная литература:

№ п/п	Источник
1	**Ищейнов, Вячеслав Яковлевич**. Защита конфиденциальной информации / В.Я. Ищейнов, М.В. Мецатунян.– М.: ФОРУМ, 2009.– 254 с.
2	**Некраха, Андрей Вячеславович**. Организация конфиденциального делопроизводства и защита информации / А.В. Некраха, Г.А. Шевцова.– М.: Академический Проект, 2007.– 219 с.
3	**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.
4	**Астанин, Иван Константинович**. Защита информации / И.К. Астанин, Н.И. Астанин.– Воронеж: Воронеж. гос. ун-т, 2006.– с.169

б) дополнительная литература:

№ п/п	Источник
5	**Краковский, Ю.М.** Информационная безопасность и защита информации / Ю.М. Краковский.– М.: Ростов н/Д: МарТ, 2008.– 287 с.
6	**Галицкий, Александр Владимирович**. 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, Людмила Клементьевна**. 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, Александр Васильевич**. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин.– М.: Академия, 2009.– 271 с.
9	**Аграновский, Александр Владимирович**. Практическая криптография: Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади.– М.: СОЛОН-Пресс, 2002.– 254с.
10	**Живетин, Владимир Борисович**. 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	*Поисковые системы www.google.ru www.yandex.ru*

14. Материально-техническое обеспечение дисциплины:

Учебные аудитории для проведения лекционных и лабораторных занятий. Компьютерные классы для выполнения индивидуальных заданий, оснащённые лицензионным и свободно распространяемым программным обеспечением.

15. Методические рекомендации по организации изучения 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.
6. Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала с разбором основных типовых задач, имеется зачёт по контрольной работе.

16. Критерии оценки видов аттестации по итогам освоения дисциплины:

В результате освоения дисциплины 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; криптографические стандарты; защитные механизмы и средства обеспечения сетевой безопасности.

- Уметь: классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; работать с интегрированной средой разработки программного обеспечения; применять средства антивирусной защиты и обнаружения вторжений; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

- Владеть: навыками настройки межсетевых экранов; методикой анализа сетевого трафика; методикой анализа результатов работы средств

обнаружения вторжений; методами и средствами выявления угроз безопасности компьютерным системам.

16.1 Критерии оценок при сдаче экзамена

16.2 Критерии оценок при сдаче зачета

Зачтено. Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;

Незачтено. Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете.