

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

УТВЕРЖДАЮ
декан факультета прикладной
математики, информатики
и механики
А.И. Шашкин
24.06.2021



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.44 Защита программ и данных

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация: Анализ безопасности компьютерных систем

Математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Сафронов В. В., кандидат технических наук, доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики
15.06.2021 г., протокол №10

8. Учебный год: 2024/2025

Семестр(ы): 8

9. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Защита программ и данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

10. Место учебной дисциплины в структуре ООП: Дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

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

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения	
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.14	знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов.	
		ОПК-5.15	знает организацию защиты информации от утечки по техническим каналам на объектах информатизации		Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем.
		ОПК-5.16	знает возможности технических средств перехвата информации		Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
ОПК-7	Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	ОПК-7.5	умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач	Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем.	
		ОПК-7.6	владеет навыками разработки, документирования, тестирования и отладки программ		Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем.
		ОПК-7.9	знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения		Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.
		ОПК-7.10	умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач;		Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем.
ОПК-13	Способен разрабатывать компоненты программных	ОПК-13.18	Умеет применять средства и методы анализа программного обеспечения для выявления закладок	Владение современными программно-аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая	

	и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности ;	ОПК-13.19	Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем.	защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
		ОПК-13.20	Знает программные методы предотвращения несанкционированного доступа к данным.	
		ОПК-13.21	Уметь применять современные средства обеспечения информационной безопасности программ и данных	
		ОПК-13.22	Знает основные программные методы защиты данных от несанкционированного доступа	
		ОПК-13.23	Умеет проводить анализ программных средств, применяемых для контроля и защиты информации	
		ОПК-13.24	Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации	
ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.11	Знает основные виды деструктивных воздействий на программные продукты.	
		ОПК-16.12	Умеет выявлять действие вредоносных программ, и определять характер их воздействия.	
		ОПК-16.13	Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем.	

12. Объем дисциплины в зачетных единицах/час (в соответствии с учебным планом) — 3/108.

Форма промежуточной аттестации (зачет/экзамен) ЭКЗАМЕН.

13. Виды учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		8 семестр		
Аудиторные занятия	42	42		
в том числе:	лекции	28		
	практические	0		
	лабораторные	14		
Самостоятельная работа	30	30		
Форма промежуточной аттестации (зачет – 0 час. / экзамен – час.)	0/36	0/36		
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	Аппаратные и программные методы защиты данных и программ	Защита данных и программ с помощью шифрования.	Защита программ и данных (10.05.01)
1.2	Защита от несанкционированного доступа в ОС	Система безопасности и разграничения доступа к ресурсам в ОС. Файловые системы и сервисы ОС Windows.	
1.3	Защита от несанкционированного копирования	Методы простановки не копируемых меток, настройка устанавливаемой программы на конкретный компьютер, настройка на конфигурацию оборудования.	
1.4	Защита от разрушающих программных воздействий	Вредоносные программы и их классификация. Загрузочные и файловые вирусы, программы-закладки. Методы обнаружения и удаления вирусов, восстановления программного обеспечения.	
1.5	Защита данных в базах данных	Основные средства защиты данных в БД: - вход по паролю: для начала работы с БД необходимо ввести определенную комбинацию символов; - разграничение прав доступа к объектам БД; защита полей и строк таблиц БД; - поддержание целостности данных; - поддержание СУБД концепции владельца данных; - шифрование данных.	
1.6	Защита информации в вычислительных сетях	Защита информации в распространенных типах вычислительных сетей.	
2. Лабораторные работы			
2.1	Лабораторная работа №1. Аппаратные и программные методы защиты данных и программ.	<i>Теоретические сведения</i> 1. Классификация методов защиты. 2. Юридические аспекты защиты. 3. Классификация методов шифрования. 4. Обзор различных алгоритмов шифрования. 5. Аппаратные средства защиты. 6. Физические средства защиты. Системы разграничения доступа. <i>Практическая часть</i> 1. Реализовать программно некоторые рассмотренные алгоритмы.	
2.2	Лабораторная работа №2. Защита от несанкционированного доступа в ОС.	<i>Теоретические сведения</i> 1. Разделение доступа. 2. Политика безопасности. Модели и типы. 3. Аутентификация. Типы. <i>Практическая часть</i> 1. Смоделировать указанный тип политики безопасности. 2. Выполнить программную реализацию одного из методов аутентификации.	
2.3	Лабораторная работа №3. Защита от несанкционированного копирования.	<i>Теоретические сведения</i> 1. Методы простановки не копируемых меток. 2. Настройка устанавливаемой программы на конкретный компьютер. 3. Настройка устанавливаемой программы на конфигурацию оборудования. 4. Юридические средства защиты от НСК. <i>Практическая часть</i> Выполнить один из пунктов примерного списка: 1. Выполнить обзор законодательных мер защиты от	

1	Аппаратные и программные методы защиты данных и программ	4	0	2	4	2	12
2	Защита от несанкционированного доступа в ОС	6	0	4	4	8	22
3	Защита от несанкционированного копирования	4	0	2	4	6	16
4	Защита от разрушающих программных воздействий	4	0	2	4	6	16
5	Защита данных в БД	8	0	4	4	8	24
6	Защита информации в вычислительных сетях	6	0	2	4	6	18
	Итого:	32	0	16	24	36	108

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, итоговое повторение теоретического материала. Подготовка к лабораторным работам, контрольной работе и экзамену.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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	Смарт, Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо .— М. : Техносфера, 2006 .— 525 с. : ил
2	Основы криптографии : [учебное пособие для студ. вузов, обуч. по группе специальностей в обл. информ. безопасности] / А.П. Алферов [и др.] .— 3-е изд., испр. и доп. — Москва : Гелиос АРВ, 2005 .— 479 с.
3	Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. :

б) дополнительная литература:

№ п/п	Источник
1	Информатика: проблемы, методология, технологии [Электронный ресурс] : материалы XVI Международной научно-методической конференции, Воронеж, 11-12 февраля 2016 г. [Секции 7-12]. Интеллектуальные информационные системы. Распределенные вычисления. Поискные методы. Компьютерная лингвистика. Квантовые информационные системы, квантовые алгоритмы, квантовая криптография. САПР и цифровые технологии / Воронеж. гос. ун-т ; под ред. Н.А. Тюкачева .— Электрон. текстовые дан. — Воронеж : Научно-исследовательские публикации, 2016 .
2	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. , обуч. по специальности "Информационные системы и технологии" днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс)
3	Ишейнов, Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В.Я. Ишейнов, М.В. Мещатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил
4	Защита данных геоинформационных систем / Л.К. Бабенко [и др.] ; [под ред. И.Г. Журкина] .— М. : Гелиос АРВ, 2010 .— 336 с. : ил.,
5	Борисова, С.Н. Методы и средства криптографической защиты данных в вычислительных системах. Часть 2. [Электронный ресурс] : Учебные пособия — Электрон. дан. — Пенза : ПензГТУ, 2013. — 107 с. — Режим доступа: http://lanbook.lib.vsu.ru/book/62779

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

№ п/п	Ресурс
1.	https://e.lanbook.com/ - ЭБС «Лань»

2.	www.lib.vsu.ru — Зональная научная библиотека ВГУ
3.	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] : Учебные пособия / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://lanbook.lib.vsu.ru/book/1540 — Загл. с экрана.
4.	Защита программ и данных (10.05.01) /Ю.А. Крыжановская. — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru .

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

Предусмотрено получение консультаций по вопросам изучаемой дисциплины, изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, выполнение индивидуальных и групповых заданий лабораторных работ, итоговое повторение теоретического материала. Также к СРС относится подготовка к контрольной работе и экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия, методические указания по выполнению лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

№ п/п	Источник
1	Краковский, Ю.М. Информационная безопасность и защита информации : учебное пособие для студ. , обуч. по специальности "Информационные системы и технологии" днев. и заоч. форм обучения / Ю.М. Краковский .— М. : Ростов н/Д : МарТ, 2008 .— 287 с. : ил.— (Учебный курс)
2	http://dic.academic.ru/dic.nsf/ruwiki/200171 - Средства защиты информации

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

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, обозначение теоретического и практического компонентов в учебном материале. Применяются разные типы лекций (вводная, обзорная, информационная, проблемная). Дисциплина реализуется с применением информационно-коммуникационных технологий.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle).

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория должна быть оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном. Лаборатория должна быть оснащена современными компьютерами. Число компьютеров должно быть таким, чтобы обеспечивалась индивидуальная работа студентов. Для организации самостоятельной работы необходима учебная аудитория с персональными компьютерами с доступом в сеть «Интернет» и к платформе Электронного университета ВГУ.

Программное обеспечение:

OS Windows 8(10), Microsoft Visual Studio Community, PHPMyAdmin, MS SQL Server.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Аппаратные и программные методы защиты данных и программ Защита от несанкционированного доступа в ОС	ОПК-5 ОПК-7 ОПК-13 ОПК-16	ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-7.5; ОПК-7.6; ОПК-7.9; ОПК-7.10; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-16.11; ОПК-16.12; ОПК-16.13	устный опрос, контрольная работа, лабораторные работы
2	Защита от несанкционированного копирования			
3	Защита от разрушающих программных воздействий			
4	Защита данных в базах данных			
5	Защита информации в вычислительных сетях			
6	Аппаратные и программные методы защиты данных и программ			
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов

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:

- устный опрос,
- контрольная работа,
- лабораторные работы.

Перечень вопросов устного опроса

1. Классификация основных методов шифрования.
2. Шифрование на основе линейных сдвиговых регистров с обратной связью.
3. SQL-инъекции. Методы защиты.
4. Симметричное шифрование.
5. Алгоритм Диффи-Хэллмана.
6. Асимметричное шифрование.
7. Сетевая аутентификация.
8. Усиленная аутентификация на основе сертификатов.
9. Вирусы.
10. Классификация вирусов.
11. Средства антивирусной защиты. Согласование параметров SSL при установлении связи
12. Криптографические методы, используемые в SSL.
13. Формат пакета ESP.
14. Протокол Oakley.
15. Протокол почтовых сообщений MIME, S/MIME.
16. Кодировки MIME.
17. Теоретико-числовые алгоритмы, лежащие в основе шифрования с открытым ключом.
18. Точка доступа, беспроводные адаптеры сети WiFi.
19. Использование сертификатов S/MIME
20. Построение безопасных web-страниц.
21. Настройки безопасности в сервере Apache.
22. PhpMyAdmin.

23. Угрозы нарушения защиты web.
24. Протокол расширенной аутентификации Kerberos.
25. ЭЦП.
26. Свойства и правовые основы ЭЦП.
27. Алгоритмы создания и проверки ЭЦП.
28. Хэш-функции.
29. Алгоритмы хэширования.
30. Свойства популярных брандмауэров.
31. Математические основы криптографии.
32. Фильтрация трафика.
33. Управление ключами IpSec.
34. Создание защищенной БД в MS SQLServer.
35. Настройки безопасности в сервере IIS6.
36. Юридические аспекты защиты программ и данных.
37. Использование встроенных средств контроля значений данных в БД в соответствии с типами.
38. Система безопасности и разграничения доступа к ресурсам в ОС.
39. Списки контроля доступа.
40. Авторизация в доменах Windows.
41. Защита от несанкционированного копирования.
42. Изоляция процессов в современных ОС.
43. Брандмауэры. Сетевые фильтры.
44. Сетевые атаки. Методы защиты.
45. Защита сетей GSM.
46. Восстановление ПО после вирусной атаки

Перечень заданий для контрольных работ

Вариант 1.

1. Алгоритм Диффи-Хэлламана.
2. Сетевая аутентификация.
3. Вирусы.
4. Построение безопасных web-страниц.
5. Настройки безопасности в сервере Apache.
6. PhpMyAdmin.

Вариант 2.

1. Математические основы криптографии.
2. Фильтрация трафика.
3. Управление ключами IpSec.
4. Создание защищенной БД в MS SQLServer.
5. Настройки безопасности в сервере IIS6.
6. Восстановление ПО после вирусной атаки

20.2 Промежуточная аттестация

Перечень вопросов к экзамену

1. Классификация основных методов шифрования.
2. Шифрование на основе линейных сдвиговых регистров с обратной cdzpm.
3. SQL-инъекции. Методы защиты.
4. Симметричное шифрование.
5. Алгоритм Диффи-Хэлламана.
6. Асимметричное шифрование.
7. Сетевая аутентификация.

8. Усиленная аутентификация на основе сертификатов.
9. Вирусы.
10. Классификация вирусов.
11. Средства антивирусной защиты.Согласование параметров SSL при установлении связи
12. Криптографические методы, используемые в SSL.
13. Формат пакета ESP.
14. Протокол Oakley.
15. Протокол почтовых сообщений MIME, S/MIME.
16. Кодировки MIME.
17. Теоретико-числовые алгоритмы, лежащие в основе шифрования с открытым ключом.
18. Точка доступа, беспроводные адаптеры сети WiFi.
19. Использование сертификатов S/MIME
20. Построение безопасных web-страниц.
21. Настройки безопасности в сервере Apache.
22. PhpMyAdmin.
23. Угрозы нарушения защиты web.
24. Протокол расширенной аутентификации Kerberos.
25. ЭЦП.
26. Свойства и правовые основы ЭЦП.
27. Алгоритмы создания и проверки ЭЦП.
28. Хэш-функции.
29. Алгоритмы хэширования.
30. Свойства популярных брандмауэров.
31. Математические основы криптографии.
32. Фильтрация трафика.
33. Управление ключами IpSec.
34. Создание защищенной БД в MS SQLServer.
35. Настройки безопасности в сервере IIS6.
36. Юридические аспекты защиты программ и данных.
37. Использование встроенных средств контроля значений данных в БД в соответствии с типами.
38. Система безопасности и разграничения доступа к ресурсам в ОС.
39. Списки контроля доступа.
40. Авторизация в доменах Windows.
41. Защита от несанкционированного копирования.
42. Изоляция процессов в современных ОС.
43. Брандмауэры. Сетевые фильтры.
44. Сетевые атаки. Методы защиты.
45. Защита сетей GSM.
46. Восстановление ПО после вирусной атаки

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторных работ; контрольной работы. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по защите программ и данных.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.