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

УТВЕРЖДАЮ

Заведующий кафедрой
информационных систем
доцент Борисов Д.Н.,
28.02.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ФТД.В.01 Методы защиты информационных систем
Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализация: *Анализ и синтез информационных систем, Информационные технологии в менеджменте, Мобильные приложения и компьютерные игры, Системы прикладного искусственного интеллекта*

3. Квалификация выпускника: *Магистр*

4. Форма обучения: *Очная*

5. Кафедра, отвечающая за реализацию дисциплины: *информационных систем*

6. Составители программы: Борисов Дмитрий Николаевич, к.т.н., доцент, Головкин Александр Алексеевич, ассистент

ная степень, ученое звание)

_____
_____

7. Рекомендована: _НМС ФКН, протокол № 3 от 25.02.2022.
(наименование рекомендующей структуры, дата, номер протокола,
_____
отметки о продлении вносятся вручную)

8. Учебный год:___ 2022-2023_____ **Семестр(ы):** ___1__

9.Цели и задачи учебной дисциплины
Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- *понимание основных аспектов и методов защиты информационных систем;*
- *изучение принципов работы компонентов защиты информационных систем;*
- *изучение предъявляемых требований и мер, необходимых для обеспечения защиты информационных систем;*

Задачи учебной дисциплины:

- *приобретение практических навыков проектирования защиты информационных систем согласно требованиям законодательства Российской Федерации.*

10. Место учебной дисциплины в структуре ООП дисциплина относится к дисциплинам, формируемым участниками образовательных отношений. Факультативы. Требуется предварительное знание информатики, введение в программирование.

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	Знать: современные информационно-коммуникационные и интеллектуальные технологии: основные стадии разработки, принцип декомпозиции задач, возможности современных программных сред и специализированных библиотек для разработки программных средств защиты конфиденциальности информации, контроля целостности данных.
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.2 Умеет обосновывать выбор современных информационно-коммуникационных интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач.	уметь: обосновывать выбор современных информационно-коммуникационных интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач
ОПК-3 Способен анализировать профессиональную информацию, выделять в ней главное,	ОПК-3.1 Знает принципы, методы и средства анализа и структурирования профессиональной информации	Знать: принципы работы основных средств защиты информации, протоколы, интерфейсы и форматы обмена данными

структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями		

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

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	№ сем. 1	Всего
Аудиторные занятия	36	36
лекции	18	18
практические	0	0
лабораторные	18	18
Самостоятельная работа	36	36
Форма промежуточной аттестации *(зачет – час..)*	зачет	
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	Основы защиты информационных систем	Основные характеристики информационной системы (ИС). Виды защищаемой информации в ИС.	
1.2	Законодательство в сфере защиты ИС	149-ФЗ, 187-ФЗ, 98-ФЗ, основные документы ФСТЭК и ФСБ в сфере защиты ИС.	
1.3	Требования по обеспечению безопасности ИС	Набор требований, определяющих выбор мер защиты ИС. Обоснование архитектуры и используемых технологий в ИС	
1.4	Идентификация и аутентификация, управление доступом	Идентификация. Аутентификация и управление доступом в ИС. Модели управления доступом.	
1.5	Защита сети	МЭ, VPN/СКЗИ, прокси, IDS, IPS.	
1.6	Антивирусная защита	Антивирусная защита рабочих станций, серверов, сервисов.	
1.7	Превентивные меры защиты	Сканирование на наличие уязвимостей. Противодействие разведке. Контроль и установка обновлений.	
1.8	Контроль действий и регистрация событий ИБ	Контроль действий пользователей и администраторов. События безопасности. Регистрация событий безопасности.	

1.9	Защита виртуальных сред, эшелонирование защиты	Защита виртуальных сред. Резервное копирование. Эшелонирование защиты.	
2. Лабораторные занятия			
2.1	Настройка идентификации и аутентификации	Настройка идентификации и аутентификации на операционных системах АРМ и серверов, сетевого оборудования.	
2.2	Управление доступом ч. 1	Управление доступом в операционных системах на базе Linuxи Windows.	
2.3	Управление доступом ч. 2	Управление доступом в ОС и ПО сетевого оборудования и средств защиты.	
2.4	Защита сети ч. 1	Настройка межсетевого экрана на базе ACL, настройка защищённого VPN-соединения клиент-сервер.	
2.5	Защита сети ч. 2	Установка и базовая настройка Suricata.	
2.6	Антивирусная защита	KES, KSM.	
2.7	Превентивные меры защиты	Сканирование сетей. Анализ сетевого трафика.	
2.8	Превентивные меры защиты ч. 2	Знакомство с Honeypot.	
2.9	Регистрация событий ИБ	Знакомство с системой мониторинга Zabbix.	

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	Основы защиты информационных систем	2		1		4
2	Законодательство в сфере защиты ИС	2		1		4
3	Требования по обеспечению безопасности ИС	2		1		4
4	Идентификация и аутентификация, управление доступом	2		4		4
5	Защита сети	2		3		4
6	Антивирусная защита	2		1		4
7	Превентивные меры защиты	2		3		4
8	Контроль действий и регистрация событий ИБ	2		2		4
9	Защита виртуальных сред, эшелонирование защиты	2		2		4
	Итого	18		18	36	72

14. Методические указания для обучающихся по освоению дисциплины

Студентам читать рекомендованную литературу, во время проверки выполнения лабораторных работ, преподавателю рекомендуется проводить теоретический опрос с целью определения степени усвоения материала.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный*

	// Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032
2	*Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий : учебное пособие / В. А. Сердюк. — Москва : Высшая школа экономики, 2011. — 572 с. — ISBN 978-5-7598-0698-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/66085*
3	*Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103200*

б) дополнительная литература:

№ п/п	Источник
3	*Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401*
4	*Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М. А. Иванов, И. В. Чугунков. — Москва : НИЯУ МИФИ, 2012. — 400 с. — ISBN 978-5-7262-1676-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/75810*
5	*Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100522*
6	*Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844*
7	*Технические средства и методы защиты информации : учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва : Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154*
8	*Буранова, М. А. Комплексная система защиты информации : учебное пособие / М. А. Буранова, Н. В. Киреева. — Самара : ПГУТИ, 2019. — 145 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223181*

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

№ п/п	Ресурс
9	www.lib.vsu.ru – *ЗНБ ВГУ*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	*Фот, Ю. Д. Методы защиты информации : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159977*
2	*Комплексные системы защиты информации на предприятиях : учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома : КГУ им. Н.А. Некрасова, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/201884*
3	*Нестандартные методы защиты информации : учебное пособие / составители В. П. Пашинцев, А. В. Ляхов. — Ставрополь : СКФУ, 2016. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155239*

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

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

---

18. Материально-техническое обеспечение дисциплины:

1) лекционная аудитория, оснащенная мультимедиа проектором;

2) класс для проведения практических занятий;

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Раздел дисциплины (модуля)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Требования по обеспечению безопасности ИС	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	Контрольная работа 1
2	Превентивные меры защиты	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	Контрольная работа 2
3	Защита виртуальных сред, эшелонирование защиты	ОПК-2, ОПК-3	ОПК-2.1, ОПК-2.2, ОПК-3.1	Контрольная работа 3

Промежуточная аттестация

Форма контроля – зачет

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

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 (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на лекционных занятиях;

Контрольная работа по теоретической части курса;

Лабораторные работы.

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	Устный опрос на практических занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по	Теоретические вопросы по темам/разделам	Шкала оценивания соответствует

	разделам дисциплины	дисциплины	приведенной ниже
3	Лабораторная работа	Содержит 9 лабораторных заданий, предусматривающих настройку и эксплуатацию различных средств защиты информации.	При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.

Пример задания для выполнения практической работы

Контрольная работа 1

Вариант 1

1) Определение характеристик информационной системы;

2) Набор требований, определяющих выбор мер защиты ИС;

3) Обоснование архитектуры и используемых технологий в ИС;

Примеры вопросов из теста:

Тестовый вопрос: Какой документ ФСТЭК определяет требования к защите информации в АСУ ТП

Варианты ответа:

1) Приказ ФСТЭК №21

2) Приказ ФСТЭК №31

3) Приказ ФСТЭК №17

Тестовый вопрос: Что является основным документом, регламентирующим использование средств криптографической защиты информации

Варианты ответа:

1) ФЗ-187

2) ФЗ-149

3) Приказ ФСБ №378

4) Приказ ФСТЭК №31

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня практических работ, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Соотношение показателей, критериев и шкалы оценивания результатов обучения представлено в следующей таблице.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, выполнение заданий, предусмотренных программой, знакомство с основной литературой,		*Зачет*

рекомендованной программой. Присутствуют погрешности в ответе на экзамене и при выполнении экзаменационных заданий.		
Имеются пробелы в знаниях основного учебно-программного материала, принципиальные ошибки в выполнении предусмотренных программой заданий, наличие которых препятствует дальнейшему обучению студента.		*Не зачет*

КИМ формируется из трех теоретических вопросов и одной практической задачи.

Перечень вопросов к зачету:

1. Основные характеристики информационной системы (ИС). Виды защищаемой информации в ИС.
2. 149-ФЗ, 187-ФЗ, 98-ФЗ, основные документы ФСТЭК и ФСБ в сфере защиты ИС.
3. Набор требований, определяющих выбор мер защиты ИС. Обоснование и регламентация используемых технологий в ИС.
4. Идентификация. Аутентификация и управление доступом в ИС.
5. Модели управления доступом.
6. Межсетевые экраны, VPN, прокси-серверы.
7. Системы обнаружения и предотвращения вторжений.
8. Антивирусная защита рабочих станций, серверов, сервисов.
9. Сканирование на наличие уязвимостей. Противодействие разведке.
10. Контроль и установка обновлений.
11. Контроль действий пользователей и администраторов.
12. События безопасности. Регистрация событий безопасности.
13. Защита виртуальных сред.
14. Резервное копирование.
15. Эшелонирование защиты.
16. Формирование документа, определяющего перечень мер, необходимых для обеспечения безопасности информации на основе предъявляемых требований.
17. Формирование документов, определяющих выбор средств защиты информации и состав их функций, реализующих меры по обеспечению защиты информации.
18. Формирование документов, содержащих описание настроек средств защиты информации, порядок действий для проверки функционирования средств защиты и их настроек.
19. Формирование программы и методики испытаний, документа оценки эффективности принятых мер, ввод в действие системы защиты информации.