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

УТВЕРЖДАЮ

Заведующий кафедрой
информационных систем
доцент Борисов Д.Н.,
05.05.2025

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: *Программные технологии в инфокоммуникационных системах*

3. Квалификация выпускника: *Магистр*

4. Форма обучения: *Заочная*

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

6. Составители программы: Борисова Алла Александровна, к.и.н., доцент,

(ФИО, ученая степень, ученое звание)

_____
_____

7. Рекомендована: НМС ФКН, протокол № 7 от 05.05.2025
(наименование рекомендующей структуры, дата, номер протокола,
_____
отметки о продлении вносятся вручную)

8. Учебный год: 2026-2027 **Триместр(ы):** 5 триместр, 2курс

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
ПК-5 Способен описывать и сопровождать архитектуру вычислительных систем и комплексов, обеспечивает их работоспособность и безопасность	ПК-5.1 администрирует встроенные подсистемы и средства защиты информации	Уметь: администрировать встроенные подсистемы и средства защиты информации

12. Объем дисциплины в зачетных единицах/час — *1 / 36*

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	Триместр 5	Всего
Аудиторные занятия	12	12
лекции	6	6
практические	0	0
лабораторные	6	6
Самостоятельная работа	24	24
Форма промежуточной аттестации *(зачет – час..)*	зачет	
Итого:	36	36

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 Законодательство в сфере защиты ИС	Основные характеристики информационной системы (ИС). Виды защищаемой информации в ИС. 149-ФЗ, 187-ФЗ, 98-ФЗ, основные документы ФСТЭК и ФСБ в сфере защиты ИС.	https://edu.vsu.ru/course/view.php?id=31694
1.2	Требования по обеспечению безопасности ИС	Набор требований, определяющих выбор мер защиты ИС. Обоснование архитектуры и используемых технологий в ИС	https://edu.vsu.ru/course/view.php?id=31694
1.3	Идентификация и аутентификация, управление доступом	Идентификация. Аутентификация и управление доступом в ИС. Модели управления доступом.	https://edu.vsu.ru/course/view.php?id=31694
1.4	Защита сети	МЭ, VPN/СКЗИ, прокси, IDS, IPS.	https://edu.vsu.ru/course/view.php?id=31694
1.5	Антивирусная защита	Антивирусная защита рабочих станций, серверов, сервисов.	https://edu.vsu.ru/course/view.php?id=31694
1.6	Защита виртуальных сред, эшелонирование защиты	Защита виртуальных сред. Резервное копирование. Эшелонирование защиты.	https://edu.vsu.ru/course/view.php?id=31694
2. Лабораторные занятия			
2.1	Настройка идентификации и аутентификации	Настройка идентификации и аутентификации на операционных системах АРМ и серверов, сетевого оборудования.	https://edu.vsu.ru/course/view.php?id=31694
2.2	Управление доступом ч. 1	Управление доступом в операционных системах на базе Linuxи Windows. Управление доступом в ОС и ПО сетевого оборудования и средств защиты.	https://edu.vsu.ru/course/view.php?id=31694
2.3	Защита сети ч. 1	Настройка межсетевого экрана на базе ACL, настройка защищённого VPN-соединения клиент-сервер. Установка и базовая настройка Suricata	https://edu.vsu.ru/course/view.php?id=31694
2.4	Антивирусная защита	KES, KSM.	https://edu.vsu.ru/course/view.php?id=31694
2.5	Превентивные меры защиты	Сканирование сетей. Анализ сетевого трафика. Знакомство с Honeypot.	https://edu.vsu.ru/course/view.php?id=31694
2.6	Регистрация событий ИБ	Знакомство с системой мониторинга Zabbix.	https://edu.vsu.ru/course/view.php?id=31694

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. Законодательство в сфере защиты ИС	1			4	5
2	Требования по обеспечению безопасности ИС	1		2	4	7
3	Идентификация и аутентификация, управление доступом	1			4	5
4	Защита сети	1		2	4	7
5	Антивирусная защита	1			4	5
6	Защита виртуальных сред, эшелонирование защиты	1		2	4	7
	Итого	6		6	24	36

14. Методические указания для обучающихся по освоению дисциплины

Внеаудиторная самостоятельная работа студентов включает проработку материалов лекций, изучение рекомендованной литературы, подготовку к лабораторным работам и их защитам, подготовку к устному опросу и зачету.

Самостоятельная работа в аудитории выполняется под непосредственным руководством преподавателя. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Для повышения эффективности руководства при проведении лабораторных занятий, призванных обеспечить выборочное использование лекционного материала для более глубокого изучения отдельных разделов дисциплины при решении соответствующих практических задач.

К лабораторным занятиям студенты должны изучить теоретический материал предметной области, основы программирования на языке С.

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

а) основная литература:

№ п/п	Источник
1	*Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279*
2	*Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/326153*
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*
4	*Ванюшина, А. В. Основы информационной безопасности : учебно-методическое пособие / А. В. Ванюшина, С. Ю. Рыбаков. — Москва : МТУСИ, 2022. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/333701*

б) дополнительная литература:

№ п/п	Источник
1	*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
2	*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*
3	*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*
4	*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
1	www.lib.vsu.ru – *ЗНБ ВГУ*
	Электронно-библиотечная система «Лань», https://reader.lanbook.com

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; ауд. 479 1) Мультимедийная лекционная аудитория: компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19", мультимедийный проектор, экран, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) класс для проведения практических занятий (компьютерный класс) (одна из №1-4 корп. 1а, ауд. № 382-385), Учебная аудитория: специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24'' (16 шт.), специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

---

19. Оценочные средства для проведения текущей и промежуточной аттестаций

При текущей аттестации используется шкала «зачтено – не зачтено» со следующими критериями оценок:

- «зачтено» – выставляется, если студент выполняет лабораторные работы в соответствии с заданием, не допуская ошибок, или обнаруживает и исправляет их в ходе представления результатов выполнения задания.

- «не зачтено» – выставляется, если студент не выполнил работу или допустил принципиальные ошибки при выполнении задания.

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	ПК-5	ПК-5.1	Лабораторная работа 1, тестовое задание
2	Превентивные меры защиты	ПК-5	ПК-5.1	Лабораторная работа 2
3	Защита виртуальных сред, эшелонирование защиты	ПК-5	ПК-5.1	Лабораторная работа 3 Тестовое задание

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 (лабораторные работы и тестирования). 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;

Лабораторные работы;

Тестирование

Текущая аттестация проводится в течение всего обучения в рамках освоения дисциплины и заключается в выполнении студентом 3-х лабораторных работ, успешного прохождения тестовых заданий (не менее 50 % правильных ответов), а также успешного написания контрольной работы (получение не менее 50 баллов из 100 баллов). Тестовые задания выполняются студентами после прослушивания лекций; лабораторные работы выполняются в течении отчетной сессии, но не позже итоговой аттестации. Контрольная работа выполняется после предоставления отчетов по трем лабораторным работам.

Лабораторные работы после выполнения оцениваются преподавателем, и выставляется оценка «зачтено» по лабораторной работе при условии ответа на 80% вопросов преподавателя по предметной области лабораторной 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
3	Лабораторная работа	Содержит 3 лабораторных задания, 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.
4	Тестирование		Выполнение 50% успешного прохождения тестовых заданий считается зачтенным

Пример задания для выполнения практической работы

Лабораторная 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

Лабораторная работа 2

Вариант 1

1. Дать определение аутентификации. Привести примеры.

2. Дать определение идентификации в информационных системах

3. Дать определение авторизации пользователя

4. Дать определение пароля

Лабораторная работа 3

Вариант 1

1. Системой криптографической защиты информации является:

а) BFox Pro

б) CAudit Pro

в) Крипто Про

2. Какие вирусы активизируются в самом начале работы с операционной системой:

а) загрузочные вирусы

б) троянцы

в) черви

3. Stuxnet — это:

а) троянская программа

б) макровирус

в) промышленный вирус

4. Таргетированная атака — это:

а) атака на сетевое оборудование

б) атака на компьютерную систему крупного предприятия

в) атака на конкретный компьютер пользователя

Приведенные ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний:

ПК-5

Задания закрытого типа

1. Под информационной безопасностью понимается:

а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

в) нет верного ответа

2. Защита информации:

а) небольшая программа для выполнения определенной задачи

б) комплекс мероприятий, направленных на обеспечение информационной безопасности

в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

3. Информационная безопасность зависит от:

а) компьютеров, поддерживающей инфраструктуры

б) пользователей

в) информации

4. Конфиденциальностью называется:

а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

б) описание процедур

в) защита от несанкционированного доступа к информации

5. Для чего создаются информационные системы:

а) получения определенных информационных услуг

б) обработки информации
в) оба варианта верны

6. Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

7. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

8. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

9. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности

10. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

Задания открытого типа

1. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?_____

2. Как называется попытка реализации угрозы?_____

3. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право?_____

4. Если злоумышленник внедрил в компьютер вредоносную программу и получил доступ к личной информации пользователя, какое свойство информации было нарушено?_____

5. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?_____

6. Анна послала письмо Степану. Злоумышленник уничтожил письмо Анны, подсунул свое и отправил Степану от имени Анны. Какое свойство информации было нарушено?_____

7. Анна послала письмо Степану. Злоумышленник прочитал письмо Анны, подсунул вместо него свое и отправил Степану от имени Анны. Какое свойство(а) информации было(и) нарушено?_____, _____

8. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?_____

9. Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?_____

10. Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу?_____

Задания с развернутым ответом

1. Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте восемь первых букв из своих данных: Фамилии, Имени, Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые четыре буквы.

20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение триместра), 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, рекомендованной программой. Присутствуют погрешности в ответе на зачете и при выполнении заданий.		*Зачет*
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.