Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Матвеев Александр Валерьевич
Должность: Проректор по образовательной деятельности
Дата подписания: 04.08.2026 15:06:18
Уникальный программный ключ:
287d28879a9eafccca070f6fe8b2fd87c7444eca

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Вологодский государственный университет»

УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____Матвеев А.В.
« » 2026 г.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки / специальность: 09.03.01 Информатика и вычислительная техника

Направленность (профиль / специализация): Программное обеспечение средств вычислительной техники и информационной безопасности

Квалификация выпускника: бакалавр

Форма обучения: Очная

Институт: математики, естественных и компьютерных наук

Кафедра: автоматики и вычислительной техники

Вологда
2026г.

Составитель рабочей программы
доцент, ктн, доцент _ / Тихомирова Е.Н. /

Рабочая программа дисциплины **Основы информационной безопасности** разработана в соответствии с ФГОС ВО по направлению подготовки/специальности 09.03.01 Информатика и вычислительная техника, направленность Программное обеспечение средств вычислительной техники и информационной безопасности.

Составлена на основании учебного плана направления подготовки 09.03.01 Информатика и вычислительная техника, направленность Программное обеспечение средств вычислительной техники и информационной безопасности.

Рабочая программа рассмотрена на заседании кафедры Автоматики и вычислительной техники

Заведующий кафедрой _ /Суконщиков А.А. /

Рабочая программа одобрена на заседании методического совета института МЕиКН

Протокол от «14» мая 2026 г. № 8.

Председатель методического совета /Голубев О.Б./

СОГЛАСОВАНО:

Председатель рабочей группы
по УГНС 09.00.00 _ / Суконщиков А.А./

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины являются

1. формирование у студентов знаний и представлений о смысле, целях и задачах информационной безопасности, характерных свойствах защищаемой информации, основных информационных угрозах, существующих (действующих) направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

2. обучение студентов принципам обеспечения информационной безопасности государства, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем.

3. приобретение практических навыков в области создания систем защиты информации

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ УЧЕБНОГО ПЛАНА

Дисциплина относится к дисциплинам обязательной части блока Б1.

Требования к предварительной подготовке обучающегося: основные понятия и аксиомы информатики, методы, устройство ЭВМ и основные методы и приемы работы с персональным компьютером, основные методы и приемы работы вычислительными сетями. Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее: комплексная защита информации, управление информационной безопасностью

Освоение дисциплины возможно с применением электронного обучения и дистанционных образовательных технологий.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-7. Способен участвовать в настройке и наладке программно-аппаратных комплексов
ОПК-7.1. Изучает методику настройки и наладки программно-аппаратных комплексов
ОПК-7.2. Осуществляет настройку и наладку программно-аппаратных комплексов
ОПК-7.3. Участвует в настройке и наладке программно-аппаратных комплексов
ПК-1 Способен разрабатывать требования и проектировать программное обеспечение
ПК-1.1. Изучает требования к программному обеспечению
ПК-1.2. Осуществляет проектирование программного обеспечения
ПК-1.3. Формирует сборку модулей и компонент программного обеспечения

В результате освоения дисциплины обучающийся должен:

знать:

- свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность,
- основное содержание, средства и методы используемых на практике или развиваемых направлений информационной защиты,
- основные принципы, стратегии и модели информационной защиты,
- наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий, и типичные качества личности преступников,
- составы преступлений в сфере компьютерной информации, предусмотренные УК РФ, и толкование специальных терминов, употребляемых в них,
- принципы комплексирования средств и методов защиты информации.

уметь:

- Правильно проводить анализ угроз информационной безопасности,
- выполнять основные этапы решения задач информационной безопасности,
- применять на практике основные общеметодологические принципы теории информационной безопасности.
- Отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

владеть/быть в состоянии продемонстрировать:

- способность и готовность выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;
- способность и готовность к анализу материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;
- способность и готовность выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

Общая трудоемкость дисциплины составляет 2 ЗЕТ (72_ часа/ов), в том числе в семестрах:

Семестр (для очной, очно-заочной)/ сессия/ курс (для заочной) №	Трудоемкость							РГР, курсовая работа, курсовой проект, контрольная работа (для заочной формы) (указывается вид работы)	Форма промежуточной аттестации
	Всего		Контактная работа			СРС	Контроль		
			час.						
	ЗЕТ	час.	Лк.	Пр.	Лаб.	час.	час.		
2/1	2	72	14		16	42			зачет

№	Наименование разделов и тем/ вид занятия	Семестр / сессия/ курс	Кол-во часов	Индикаторы достижения компетенций	Форма текущего контроля
1.	Тема: Основные понятия и задачи информационной безопасности	2/1		ПК-1, ОПК-7	
	Лекция 1: Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Актуальность проблемы обеспечения безопасности информационных технологий. Обзор защищаемых объектов и систем. Субъекты информационных	2/1	1	ПК-1, ОПК-7	

	отношений, их интересы и безопасность.				
	Лекция 2: Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика. Классификация уязвимостей и атак. Механизмы реализации атак.	2/1	1	ПК-1, ОПК-7	
	Лабораторная работа 1: Исследования влияния атак с помощью моделирующей системы	2/1	4	ПК-1, ОПК-7	Защита отчета
	СРС	2/1	10	ПК-1, ОПК-7	
2.	Тема: Основы защиты информации	2/1		ПК-1, ОПК-7	
	Лекция 3: Конфиденциальность, целостность, доступность. Пути нанесения ущерба. Цели и объекты защиты. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Цели и задачи защиты информации.	2/1	2	ПК-1, ОПК-7	
	Лекция 4: Сущность функционирования системы защиты информации. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2/1	2	ПК-1, ОПК-7	
	Лабораторная работа 2: Инструментально-моделирующий комплекс для оценки качества функционирования защищенных информационных систем.	2/1	4	ПК-1, ОПК-7	Защита отчета
	СРС	2/1	10	ПК-1, ОПК-7	
3.	Тема: Методологические подходы к защите информации	2/1		ПК-1, ОПК-7	
	Лекция 5: Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.	2/1	2	ПК-1, ОПК-7	
	СРС	2/1	5	ПК-1, ОПК-7	
4.	Тема: Нормативно правовое регулирование защиты информации	2/1		ПК-1, ОПК-7	
	Лекция 6: Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации	2/1	2	ПК-1, ОПК-7	
	Лабораторная работа 3: Исследование и анализ сетевого трафика с помощью сетевых анализаторов	2/1	4	ПК-1, ОПК-7	Защита отчета

	СРС	2/1	5	ПК-1, ОПК-7	
5.	Тема: Защита информации в информационных системах	2/1		ПК-1, ОПК-7	
	Лекция 7: Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в информационных системах	2/1	2	ПК-1, ОПК-7	
	Лекция 8: Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы Инженерная защита и техническая охрана объектов информатизации	2/1	2	ПК-1, ОПК-7	
	Лабораторная работа 4: Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.	2/1	4	ПК-1, ОПК-7	Защита отчета
	СРС	2/1	12	ПК-1, ОПК-7	
	ИТОГО		72		

5. КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

5.1. Перечень контрольных вопросов и заданий для текущего контроля представлен в Фонде оценочных средств по данной дисциплине.

5.2. Перечень контрольных вопросов и заданий для промежуточной аттестации

5.2.1 Задания для проведения промежуточной аттестации в форме зачета могут включать:

- вопросы, требующие устного или письменного ответа:

1. Основные понятия и определения в области информационной безопасности. Актуальность проблемы.
2. Классификация уязвимостей и атак. Механизмы реализации атак.
3. Цели создания системы обеспечения информационной безопасности.
4. Основные механизмы защиты компьютерных сетей.
5. Модель OSI. Сетевые протоколы.
6. Сетевые анализаторы и снифферы.

7. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.
8. Атаки на протокол ARP и его защита.
9. Атаки на протокол IP и его защита. Атаки на протокол ICMP и его защита.
10. Защита сетевого уровня. Протокол IPSEC.
11. Виртуальные частные сети. Организация VPN.
12. Защита транспортного уровня. Атаки на протокол TCP и его защита. Протоколы SSL, SSH.
13. Проблемы безопасности протоколов прикладного уровня.
14. Криптография. Основные термины. Оценка надежности криптоалгоритмов.
15. Классификация методов шифрования информации. Шифры замены. Шифры перестановки.
16. Блочные шифры. Гаммирование. Поточные шифры. Принципы построения генераторов псевдослучайных кодов.
17. Криптосистемы с секретным ключом. Модель системы и ее основные свойства.
18. Криптосистемы с открытым ключом. Модель системы и ее основные свойства.
19. Модель безопасности ОС Windows. Компоненты системы безопасности. Объекты доступа.
20. Модель безопасности СУБД. Режимы проверки прав. Получение доступа к БД.
21. Традиционные средства защиты корпоративной сети. Комплексная система защиты информации. Концепции безопасности.
22. Разработка политики сетевой безопасности. Администрирование системы безопасности

- тесты, проводимые в письменной или электронной форме.

Вопрос 1. Что такое информационная безопасность:

а) защита информации;
б) уровень обеспечения защиты несанкционированного доступа;
в) состояние защищенности о внешних и внутренних угроз;
г) контроль целостности;
д) обеспечение защиты контролируемой зоны;
е) шифрование файлов.

Вопрос 2. Назначение ЭЦП:

а) обеспечение целостности;
б) обеспечение доступности;
в) обеспечение авторства;
г) обеспечение конфиденциальности;
д) обеспечение неотказуемости.

5.2.2 Оценивание уровня сформированности индикаторов компетенций у обучающихся на соответствие их подготовки ожидаемым результатам, описание их показателей, критериев и шкал оценивания в процессе проведения промежуточной аттестации представлено в Фонде оценочных средств по данной дисциплине.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

6.1. Учебно-методическое обеспечение

Библиографическое описание по ГОСТ	Кол-во экземпляров в НБ ВоГУ
1	2
Рекомендуемая литература	
1. Артемов, А. В. Информационная безопасность [Электронный ресурс]: курс лекций/ А. В. Артемов. - Орел: МАБИВ, 2014. - 257 с.: табл., схем. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=428605	ЭБС «Университетская библиотека онлайн»
2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие/ Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557	ЭБС «Университетская библиотека онлайн»
3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ С. А. Нестеров. - Санкт-Петербург: СПбПУ, 2014. - 322 с.: схем., табл., ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=363040	ЭБС «Университетская библиотека онлайн»
4. Галатенко, В. А. Основы информационной безопасности: курс лекций: учебное пособие для вузов/ В. А. Галатенко; под ред. В. Б. Бетелина. - Москва: ИНТУИТ, 2004. - 260 с.	15
5. Галатенко, В. А. Стандарты информационной безопасности: курс лекций: для вузов/ В. А. Галатенко; под ред. В. Б. Бетелина. - Москва: ИНТУИТ, 2004. - 322 с.	5
6. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учебное пособие для вузов/ В. И. Завгородний. - Москва: Логос, 2001. - 263 с.	5
7. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft [Электронный ресурс]: практикум/ П. С. Ложников, Е. М. Михайлов. - Москва: ИНТУИТ, 2008. - 246 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=233194	ЭБС «Университетская библиотека онлайн»
8. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для вузов/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 3-е изд., стер. - Москва: Academia, 2008. - 330, [1] с. ил.	5
9. Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие/ В. И. Петренко. - Ставрополь: СКФУ, 2015. - 222 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=458204	ЭБС «Университетская библиотека онлайн»
10. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О. В. Прохорова. - Самара: СГАСУ, 2014. - 113 с.: табл., схем., ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331	ЭБС «Университетская библиотека онлайн»
11. Романец, Ю. В. Защита информации в компьютерных системах и сетях/ Ю. В. Романец, П. А. Тимофеев; В. Ф. Шаньгин. - 2-е изд., перераб. и доп. - Москва: Радио и связь, 2001. - 376 с.: ил.	4
12. Романов, О. А. Организационное обеспечение информационной безопасности: учебник для вузов/ О. А. Романов, С. А. Бабин, С. Г.	5

Жданов. - Москва: Academia, 2008. - 188, [1] с.	
13. Скрипник, Д. А. Общие вопросы технической защиты информации Электронный ресурс]: курс/ Д. А. Скрипник. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 425 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429070	ЭБС «Университетская библиотека онлайн»
14. Суконщиков, А. А. Методы и средства защиты компьютерной информации: учебное пособие по специальности "Управление и информатика в технических системах"/ А. А. Суконщиков, Е. Н. Давыдова. - Вологда: ВоГТУ, 2008. - 132 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/sukonshikov/book1/2008_sukonshikov_sash_inf.pdf	40 ЭБ ВоГУ
15. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 369 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428820	ЭБС «Университет-ская библиотека онлайн»
16. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов/ П. Б. Хорев. - Москва: Academia, 2005. - 254, [1] с.: ил.	20
17. Цирлов, В. Л. Основы информационной безопасности: краткий курс: [учебник для вузов]/ В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008. - 253, [1] с.	5
18. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс]: учебное пособие/ А. Щербаков. - Москва: Книжный мир, 2009. - 352 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=89798	ЭБС «Университетская библиотека онлайн»
19. Защита информации: методические указания к лабораторным работам: ЭЭФ: направления подготовки бакалавриата: 27.03.04 - Управление в технических системах, 09.03.01 - Информатика и вычислительная техника, 09.03.04 - Программная инженерия : профили подготовки: "Управление и информатика в технических системах", "Программное обеспечение средств вычислительной техники и автоматизированных систем", "Разработка программно-информационных систем"/ сост. Е. Н. Давыдова. - Вологда: ВоГУ, 2014. - 31 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book10/2014_davydova_zash_inf.pdf	10 ЭБ ВоГУ
20. Методы и средства защиты компьютерной информации: методические указания к практической работе № 4 "Применение механизмов QoS в системах защиты информации": ЭЭФ, ФЗДО: специальности: 220201, 230101/ [сост.: Е. Н. Давыдова, А. А. Суконщиков]. - Вологда: ВоГТУ, 2009. - 15 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book7/2009_davydova_4.pdf	29 ЭБ ВоГУ
21. Методы и средства защиты компьютерной информации: методические указания к лабораторной работе №5 "Изучение алгоритмов шифрования": ЭЭФ, ФЗДО: специальности: 220201, 230101/ [сост.: Суконщиков А. А., Давыдова Е. Н.]. - Вологда: ВоГТУ, 2009. - 11, [1] с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/sukonshikov/book4/2009_sukonshikov_sash_inf_lr5.pdf	14 ЭБ ВоГУ

6.2. Информационное обеспечение

1. Основы информационной безопасности https://www.intuit.ru/studies/courses/10/10/info
2. Введение в защиту информации от внутренних ИТ-угроз https://www.intuit.ru/studies/courses/1013/172/info
3. Доступ к учебно-методическому комплексу кафедры АВТ http://atpp.vstu.edu.ru/umk/
4. Доступ к учебно-методическому порталу ВоГУ https://do.vogu35.ru/

6.3 Программное обеспечение

1. Windows 10
2. LibreOffice

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

№№ п/п	Перечень основного оборудования
1	**2**
1.	*Персональный компьютер*
2.	*Проектор Epson EB-X10 (1 шт.)*

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в _____/ _____ учебном году на заседании кафедры Автоматики и вычислительной техники

Протокол от _____ _____ 20__ г. № __
Зав. кафедрой_

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в / учебном году на заседании кафедры

_____

Протокол от _20_ г. № _ Зав. кафедрой _

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в / учебном году на заседании кафедры

_____

Протокол от _20_ г. № _ Зав. кафедрой _

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для
исполнения в / учебном году на заседании кафедры

Протокол от _20_ г. № _ Зав. кафедрой _

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ,
ВНОСИМЫЕ В РАБОЧУЮ ПРОГРАММУ ДИСЦИПЛИНЫ

№ п/п	Содержание изменения	Основание для внесения изменений	Автор рабочей программы дисциплины, ответственный за внесение изменений	Зав.кафедрой
1.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись
2.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись
3.		протокол от «__» _20__г № _	ФИО, подпись	ФИО, подпись