Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Матвеев Александр Валерьевич
Должность: Проректор по образовательной деятельности
Дата подписания: 30.10.2026 10:48:33
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.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки / специальность: 09.03.02 Информационные системы и технологии

Направленность (профиль / специализация): Для всех профилей

Квалификация выпускника: бакалавр

Форма обучения: **заочная**
Институт: **математики, естественных и компьютерных наук**
Кафедра: **информатики и информационных технологий**

Вологда
2026 г.

Составитель рабочей программы
заведующий кафедры, ктн, доцент _____ / Суконщиков А.А. /
(должность, уч.степень, звание) *(подпись)* *(Ф. И. О.)*

Рабочая программа дисциплины « Безопасность информационных технологий и систем» разработана в соответствии с ФГОС ВО по направлению подготовки/специальности 09.03.02 – Информационные системы и технологии.
Составлена на основании учебного плана направления подготовки 09.03.02 – Информационные системы и технологии.

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 /А.А. Суконщиков/

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины являются формирование у обучающихся общепрофессиональных и профессиональных компетенций в области безопасности информационных технологий и систем при решении задач в рамках проектно-конструкторской и проектно-технологической профессиональной деятельности.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ УЧЕБНОГО ПЛАНА

Дисциплина «Безопасность информационных технологий и систем» относится к циклу обязательной части дисциплин модуля профильной направленности (Б1.О.03.20).
Требования к предварительной подготовке обучающегося: информационные технологии, аппаратное обеспечение информационных технологий, сети и телекоммуникации, теория информационных процессов и систем, архитектура информационных систем, моделирование информационных процессов и систем, инструментальные средства информационных систем, методы и средства проектирования информационных систем и технологий.

Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее: администрирование в информационных системах.
Освоение дисциплины возможно с применением электронного обучения и дистанционных образовательных технологий, в том числе на основе комбинации форматов в виде письменного решения задания (проекта).

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

ОПК-3.1 Осуществляет поиск и отбор информации о методах и средствах решения стандартных задач;
ОПК-3.2 Решает стандартные задачи на основе ИКТ и библиографической культуры;
ОПК-3.3 Осуществляет анализ и синтез полученной информации при решении стандартных задач;
ОПК-5.1 Основы администрирования программного обеспечения и информационных систем;
ОПК-5.2 Формулирует основные параметры информационных систем;
ОПК-5.3 Осуществляет параметрическую настройку информационных систем и программного обеспечения;
ОПК-5.4 Выполняет инсталляцию программного и аппаратного обеспечения, информационных систем и автоматизированных систем;
ПК-1.1 Анализирует рынок программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем;
ПК-1.2 Сопровождает информационные системы и сервисы;

В результате освоения дисциплины обучающийся должен:

знать:

- правовые основы безопасность информационных технологий и систем (ИТиС);
- математические основы криптографии;
- организационные, технические и программные методы обеспечения безопасности при эксплуатации современных ИТиС;
- стандарты, модели, методы шифрования;
- методы идентификации пользователей;
- основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;

- методы передачи конфиденциальной информации по каналам связи;
- методы установления подлинности передаваемых сообщений и хранимой информации;

уметь:

- проводить сравнительный анализ алгоритмов и методов безопасности ИТиС;
- применять методы и средства обеспечения безопасности информационных систем;

владеть/быть в состоянии продемонстрировать:

- навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации;
- навыками построения программных систем, содержащих криптографические алгоритмы шифрования передаваемой информации, алгоритмы простановки и проверки электронной цифровой подписи (ЭЦП), алгоритмы хэш-функций, алгоритмы генерации псевдослучайных последовательностей чисел.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

Общая трудоемкость дисциплины составляет 6 ЗЕТ (216 часов), 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		
	ЗЕТ	час.	час.			час.	час.		
			Лк.	Пр.	Лаб.				
5	4	144	4		12	128	36	—	Зачет, экзамен

№	Наименование разделов и тем/ вид занятия	Семестр/ сессия/ курс	Кол-во часов	Индикаторы достижения компетенций	Форма текущего контроля
1.	Тема 1. Введение.				
	Лекция 1. Задачи, цель и предмет курса. Основные понятия и определения в области безопасности ИТиС. Актуальность проблемы.	8/4	0,2	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	5	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
2.	Тема 2. Основы безопасности сетевых ИТ.				
	Лекция 2. Классификация уязвимостей и атак. Механизмы реализации атак. Цели создания системы обеспечения информационной безопасности.	8/4	0,2	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	5	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 1. Исследования влияния атак с помощью моделирующей системы.	8/4	1	ОПК-3.1	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	

	Лекция 3. Основные механизмы защиты компьютерных сетей. Идентификация и аутентификация пользователей. Регистрация и оперативное оповещение о событиях безопасности. Контроль целостности программных и информационных ресурсов. Защита периметра компьютерных сетей. Разграничение доступа. Криптографические методы защиты информации.	8/4	0,2	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 2. Инструментально-моделирующий комплекс для оценки качества функционирования защищенных информационных систем.	8/4	1	ОПК-3.2	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
3.	Тема 3. Безопасность уровня сетевого взаимодействия.				
	Лекция 4. Модель OSI. Сетевые протоколы. Сетевые анализаторы и снифферы. Защита на канальном уровне.	8/4	0,2	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 3. Исследование и анализ сетевого трафика с помощью сетевых анализаторов.	8/4	1	ОПК-3.3	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лекция 5. Протоколы PPTP, L2F, L2TP. Атаки на протокол ARP и его защита. Атаки на протокол IP и его защита. Атаки на протокол ICMP и его защита.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
4.	Тема 4. Безопасность сетевого и прикладного уровня.				
	Лекция 6. Защита сетевого уровня. Протокол IPSEC. Протоколы AH, ESP, IKE. Режимы работы IPSEC.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 4. Применение программных средств аудита безопасности ИТиС с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.	8/4	1	ОПК-5.1	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лекция 7. Виртуальные частные сети. Организация VPN. Защита транспортного уровня. Атаки на протокол TCP и его защита. Протоколы SSL, SSH. Проблемы безопасности протоколов прикладного уровня.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	

	Лабораторная работа 5. Построение моделей нарушителя и системы защиты информации с помощью сетей Петри.	8/4	1	ОПК-5.2	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
5.	Тема 5. Криптографические методы защиты информации.				
	Лекция 8. Основные термины. Оценка надежности криптоалгоритмов. Классификация методов шифрования информации. Шифры замены. Шифры перестановки. Блочные шифры. Гаммирование. Поточные шифры.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 6. Однонаправленные хэш- функции. Изучение алгоритмов электронной цифровой подписи в системах защиты информации.	8/4	1	ОПК-5.3	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лекция 9. Принципы построения генераторов псевдослучайных кодов. Криптосистемы с секретным ключом. Модель системы и ее основные свойства. Криптосистемы с открытым ключом. Модель системы и ее основные свойства.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
6.	Тема 6. Безопасность уровня операционных систем.				
	Лекция 10. Модель безопасности ОС Windows. Компоненты системы безопасности. Объекты доступа. Пользовательские пароли. Проблемы безопасности. Установки ключей реестра. Настройка системы безопасности.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 7. Инструментально-моделирующий комплекс для оценки качества функционирования защищенных информационных систем.	8/4	2	ОПК-5.4	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
7.	Тема 7. Безопасность баз данных.				
	Лекция 11. Модель безопасности СУБД. Режимы проверки прав. Получение доступа к БД. Доступ к объектам БД.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 8. Применение для защиты баз данных межсетевого экрана Firewall.	8/4	2	ПК-1.1	Защита отчета
	Самостоятельная работа. Подготовка отчета	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1,	
	о лабораторной работе.			5.2, 5.3, 5.4; ПК-1.1, 1.2	
8.	Тема 8. Обеспечение комплексной безопасности.				

	Лекция 12. Традиционные средства защиты корпоративной сети. Комплексная система защиты информации. Концепции безопасности. Разработка политики сетевой безопасности. Администрирование системы безопасности.	8/4	0,4	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Самостоятельная работа. Изучение материала лекции, чтение дополнительной литературы..	8/4	6	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	Лабораторная работа 9. Построение и моделирование комплексной системы защиты информации.	8/4	2	ПК-1.2	Защита отчета
	Самостоятельная работа. Подготовка отчета о лабораторной работе.	8/4	10	ОПК-3.1, 3.2, 3.3, 5.1, 5.2, 5.3, 5.4; ПК-1.1, 1.2	
	ИТОГО (общий объем дисциплины)		144		Экзамен
	В том числе: контактная работа		16		
	В том числе: СРС		128		
	В том числе: контроль		36		

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/экзамена могут включать:

- вопросы, требующие устного или письменного ответа;
- тесты, проводимые в письменной или электронной форме;
- письменное решение задания (проекта);
- практические задания/ задачи, требующие практического решения и ответа в письменной форме.

Перечень вопросов, требующих устного или письменного ответа:

1. Основные понятия и определения в области безопасности ИТиС. 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. 6.3. 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.

Примеры тестовых и практических заданий:
- что Вы знаете об основных механизмах защиты компьютерных сетей;
- дайте сравнительную характеристику методов шифрования информации;
- выберите меры по обеспечению политики сетевой безопасности. Обоснуйте свой выбор.

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: курс лекций/ А. В. Артемов. - Орел: МАБИВ, 2014. - 257 с. – URL: https://biblioclub.ru/index.php?page=book&id=428605	ЭБС «Университетская библиотека онлайн»
2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие/ Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с. – URL: https://biblioclub.ru/index.php?page=book&id=276557	ЭБС «Университетская библиотека онлайн»
3. Нестеров, С. А. Основы информационной безопасности: учебное пособие/ С. А. Нестеров. - Санкт- Петербург: СПбПУ, 2014. - 322 с. – URL: https://biblioclub.ru/index.php?page=book&id=363040	ЭБС «Университетская библиотека онлайн»
4. Басалова, Г. В. Основы криптографии Курс лекций / Г. В. Басалова. - Москва: ИНТУИТ, 2011. - 253 с. – URL: https://biblioclub.ru/index.php?page=book&id=233689	ЭБС «Университетская библиотека онлайн»
5. 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
6. Галатенко, В. А. Стандарты информационной безопасности: курс лекций: для вузов/ В. А. Галатенко; под ред. В. Б. Бетелина. - Москва: ИНТУИТ, 2004. - 322 с.	5
7. Завгородний, В. И. Комплексная защита информации в компьютерных системах: учебное пособие для вузов/ В. И. Завгородний. - Москва: Логос, 2001. - 263 с.	5

8. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие для вузов по специальности "Прикладная математика и информатика"/ О. Р.Лапонина; под ред. В. А. Сухомлина. - Москва: ИНТУИТ, 2005. - 605 с.	10
9. Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия: курс/ О. Р. Лапонина. - 2-е изд., исправ. - Москва: ИНТУИТ, 2016. - 462 с. - Режим доступа. – URL: https://biblioclub.ru/index.php?page=book&id=429094	ЭБС «Университетская библиотека онлайн»
10. Ложников, И. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft: практикум/ И. С. Ложников, Е. М. Михайлов. - Москва: ИНТУИТ, 2008. - 246 с. – URL: https://biblioclub.ru/index.php?page=book&id=233194	ЭБС «Университетская библиотека онлайн»
11. 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 с.	5
12. Петренко, В. И. Теоретические основы защиты информации: учебное пособие/ В. И. Петренко. - Ставрополь: СКФУ, 2015. - 222 с. – URL: https://biblioclub.ru/index.php?page=book&id=458204	ЭБС «Университетская библиотека онлайн»
13. Прохорова, О. В. Информационная безопасность и защита информации: учебник/ О. В. Прохорова. - Самара: СГАСУ, 2014. - 113 с. – URL: https://biblioclub.ru/index.php?page=book&id=438331	ЭБС «Университетская библиотека онлайн»
14. Романец, Ю. В. Защита информации в компьютерных системах и сетях/ Ю. В. Романец, И. А. Тимофеев; В. Ф. Шаньгин. - 2-е год., перераб. и доп. - Москва: Радио и связь, 2001. - 376 с.	4
15. Романов, О. А. Организационное обеспечение информационной без- опасности: учебник для вузов/ О. А. Романов, С. А. Бабин, С. Г. Жданов. - Москва: Academia, 2008. – 188 с.	5
16. Скрипник, Д. А. Общие вопросы технической защиты информации: курс/ Д. А. Скрипник. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 425 с. – URL: https://biblioclub.ru/index.php?page=book&id=429070	ЭБС «Университетская библиотека онлайн»
17. 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. – URL: http://library.vogu35.ru/biblio/sukonshikov/book1/2008_sukonshikov_sash_inf.pdf	40 ЭБ ВоГУ
18. Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. - 2-е изд., испр. - Москва: ИНТУИТ, 2016. - 369 с. – URL: https://biblioclub.ru/index.php?page=book&id=428820	ЭБС «Университетская библиотека онлайн»
19. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для вузов/ И. Б. Хорев. - Москва: Academia, 2005. - 254 с.	20 ЭБ ВоГУ
20. Цирлов, В. Л. Основы информационной безопасности: краткий курс: [учебник для вузов]/ В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008.-253 с.	5 ЭБ ВоГУ
21. Щербакова, Т. Ф. Вычислительная техника и информационные технологии: учебное пособие для вузов по направлению подготовки "Инфокоммуникационные технологии и системы связи" квалификации (степени) "бакалавр" и квалификации (степени) "магистр"/ Т. Ф. Щербакова, С. В. Козлов, А. А. Коробков. - Москва: Академия, 2012. – 301 с.	7 ЭБ ВоГУ
22. Щербаков, А. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс]: учебное пособие/ А. Щербаков. - Москва: Книжный мир, 2009. - 352 с. – URL: https://biblioclub.ru/index.php?page=book&id=89798	ЭБС «Университетская библиотека онлайн»
23. 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. – URL: http://library.vogu35.ru/biblio/davydova/book10/2014_davydova_zash_inf.pdf	10 ЭБ ВоГУ
24. Методы и средства защиты компьютерной информации: методические указания к	29

практической работе № 4 "Применение механизмов QoS в си- стемах защиты информации": ЭЭФ, ФЗДО: специальности: 220201, 230101/ [сост.: Е. Н. Давыдова, А. А. Суконщиков]. - Вологда: ВоГТУ, 2009. - 15 с. – URL: http://library.vogu35.ru/biblio/davydova/book7/2009_davydova_4.pdf	ЭБ ВоГУ
25. 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 с. – URL: http://library.vogu35.ru/biblio/sukonshikov/book4/2009_sukonshikov_sash_inf_lr5.pdf	14 ЭБ ВоГУ

6.2. Информационное обеспечение

1. Доступ к учебно-методическому комплексу кафедры АВТ http://atpp.vstu.edu.ru/umk/
2. Доступ к учебно-методическому порталу ВоГУ https://do.vogu35.ru/
3. Научная библиотека Вологодского государственного университета: электронная библиотечная система. – URL: http://library.vogu35.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст : электронный.
4. Научная электронная библиотека (НЭБ) : электронная библиотечная система. – URL: http://elibrary.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст : электронный.
5. Лань: электронная библиотечная система. – URL: https://e.lanbook.com (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст : электронный.
6. Университетская библиотека Онлайн: электронная библиотечная система. – URL: http://biblioclub.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст : электронный.
7. Znanium.com: электронная библиотечная система. – URL: http://znanium.com (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
8. IPRbooks: электронная библиотечная система. – URL: http://www.iprbookshop.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
9. Федеральный образовательный портал «Российское образование». – URL: http://www.edu.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
10. Учебные курсы Национального открытого университета «Институт». – URL: https://intuit.ru/studies/courses?page=1 (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
11. Сервер информационных технологий. – URL: http://citforum.ru (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
12. Учебные курсы Национального открытого университета «Институт»: Основы информационной безопасности. – URL: https://intuit.ru/studies/courses/10/10/info (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.
13. Учебные курсы Национального открытого университета «Институт»: Введение в защиту информации от внутренних ИТ-угроз. – URL: https://intuit.ru/studies/courses/1013/172/info (дата обращения: 01.02.2021 г.). – Режим доступа: для авториз. пользователей. – Текст: электронный.

6.3 Программное обеспечение

MS Office.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

№№ п/п	Перечень основного оборудования
1.	*Персональный компьютер/ноутбук*
2.	*Мультимедийный проектор, экран, аудиторная доска*

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 _____

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	Протокол заседания кафедры	Автор рабочей программы дисциплины, ответственный за внесение изменений	Зав.кафедрой
2.		протокол от «__» _____ 20__г № ___	ФИО, подпись	ФИО, подпись
3.		протокол от «__» _____ 20__г № ___	ФИО, подпись	ФИО, подпись
4.		протокол от «__» _____ 20__г № ___	ФИО, подпись	ФИО, подпись