Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Матвеев Александр Валерьевич
Должность: Проректор по образовательной деятельности
Дата подписания: 12.08.2026 15:34:37
Уникальный программный ключ:
287d28879a9eafccca070f6fe8b2fd87c7444eca

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

УТВЕРЖДАЮ
Проректор по образовательной
и воспитательной деятельности
_____ Матвеев А.В.
«___» _____ 2026 г.

ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки / специальность: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): для всех профилей

Квалификация выпускника: **бакалавр**

Форма обучения: **заочная**

Институт: **математики, естественных и компьютерных наук**

Кафедра: **автоматики и вычислительной техники**

Вологда
2026 г.

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

Рабочая программа дисциплины **Защита информации в автоматизированных системах** разработана в соответствии с ФГОС ВО по направлению подготовки/специальности 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА. Составлена на основании учебного плана направления подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА**.**

Рабочая программа утверждена на заседании кафедры Автоматики и вычислительной техники

Заведующий кафедрой _____ /_ Суконщиков А.А.___/

Рабочая программа одобрена на заседании методического совета института ИМЕКН

Протокол от «14» мая 2026 г. № 8.

Председатель методического совета_____ /Голубев О.Б./

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: технологии Интернет-программирования, выпускная квалификационная работа.

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

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

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

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;

ПК-1 Способен разрабатывать требования и проектировать программное обеспечение

ПК-1.1 Изучает требования к программному обеспечению;

ПК-1.2 Осуществляет проектирование ПО;

ПК-1.3 Формирует сборку модулей и компонент ПО;

ПК-5 Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем;

ПК-5.1 Основы администрирования программного обеспечения и информационных систем;

ПК-5.2 Формулирует основные параметры информационных систем;

ПК-5.3 Осуществляет параметрическую настройку информационных систем и программного обеспечения

В результате освоения дисциплины обучающийся должен:

знать:

- правовые основы защиты компьютерной информации,
- математические основы криптографии,
- организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях,
- стандарты, модели и 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 (документов, баз данных);

уметь:

- применять известные методы и средства поддержки информационной безопасности в компьютерных системах,
- проводить сравнительный анализ,

владеть/быть в состоянии продемонстрировать:

- навыками построения программных систем, использующих сервисы и механизмы безопасности, протоколы аутентификации,
- навыками построения программных систем, содержащих алгоритмы генерации псевдослучайных последовательностей чисел.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

Общая трудоемкость дисциплины составляет 6 ЗЕТ (216 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		
	ЗЕТ	час.	час.			час.	час.		
			Лк.	Пр.	Лаб.				
Зимняя/5		72	2			70			
Летняя/5	6	144			12	119	13	Курсовая работа	Зачет, экзамен

№	Наименование разделов и тем/ вид занятия	Семестр / сессия/ курс	Кол-во часов	Индикаторы достижения компетенций	Форма текущего контроля
1.	Тема: Введение			ОПК-3, ПК-1, 5	
	Лекция 1: Задачи, цель и предмет курса. Основные понятия и определения в области информационной безопасности. Актуальность проблемы.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Зимняя/5	35	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
2.	Тема: Основы безопасности сетевых информационных технологий.			ОПК-3, ПК-1, 5	
	Лекция 2: Классификация уязвимостей и атак. Механизмы реализации атак. Цели создания системы обеспечения информационной безопасности	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	Лабораторная работа 1: Исследования влияния атак с помощью моделирующей системы	Летняя/5	4	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	Защита отчета

	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.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Зимняя/5	35	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
3.	Тема: Безопасность уровня сетевого взаимодействия.			ОПК-3, ПК-1, 5	
	Лекция 4: Модель OSI. Сетевые протоколы. Сетевые анализаторы и снифферы. Защита на канальном уровне.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	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.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Летняя/5	20	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
4.	Тема: Безопасность сетевого и прикладного уровня.			ОПК-3, ПК-1, 5	
	Лекция 6: Защита сетевого уровня. Протокол IPSEC. Протоколы AH, ESP, IKE. Режимы работы IPSEC.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	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.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	Лабораторная работа 2: Построение моделей нарушителя и системы защиты информации с помощью сетей Петри.	Летняя/5	4	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	Защита отчета
	СРС	Летняя/5	20	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	

5.	Тема: Криптографические методы защиты информации.			ОПК-3, ПК-1, 5	
	Лекция 8: Основные термины. Оценка надежности криптоалгоритмов. Классификация методов шифрования информации. Шифры замены. Шифры перестановки. Блочные шифры. Гаммирование. Поточные шифры.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	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.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Летняя/5	20	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
6.	Тема: Безопасность уровня операционных систем.			ОПК-3, ПК-1, 5	
	Лекция 10: Модель безопасности ОС Windows. Компоненты системы безопасности. Объекты доступа. Пользовательские пароли. Проблемы безопасности. Установки ключей реестра. Настройка системы безопасности.	Зимняя/5	0,15	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Летняя/5	20	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
7.	Тема: Безопасность баз данных			ОПК-3, ПК-1, 5	
	Лекция 11: Модель безопасности СУБД. Режимы проверки прав. Получение доступа к БД. Доступ к объектам БД.	Зимняя/5	0,25	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	СРС	Летняя/5	20	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
8.	Тема: Обеспечение комплексной безопасности			ОПК-3, ПК-1, 5	
	Лекция 12: Традиционные средства защиты корпоративной сети. Комплексная система защиты информации. Концепции безопасности. Разработка политики сетевой безопасности. Администрирование системы безопасности.	Зимняя/5	0,25	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	Лабораторная работа 3: Построение и моделирование комплексной системы защиты информации	Летняя/5	4	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	Защита отчета
	СРС	Летняя/5	19	ОПК-3.1, 3.2, 3.3, ПК-1.1, 1.2, 1.3, ПК-5.1, 5.2, 5.3	
	ИТОГО		216		

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:

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. 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

- тесты, проводимые в письменной или электронной форме.

Пример 1:

Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

- аудит
- аутентификация
- авторизация
- идентификация

Пример 2:

Программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа

- фильтр
- заместитель

- перехватчик

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.

5.3. Курсовая работа

Цель курсовой работы состоит в формировании практических навыков проектирования комплексной системы защиты компьютерных систем.

Тема курсового проекта: Разработка системы защиты объекта информационного процесса.

Виды объектов информационных процессов

Сервер базы данных, содержащий сведения о клиентах кампании
Компьютер в бухгалтерии, под управлением Win, используемый для передачи отчетности в головной офис через VPN
Почтовый сервер крупной компании
Веб-сервер, используемый для электронной коммерции
Сервер, содержащий бухгалтерские отчеты крупной компании
Локальная сеть с выходом в Интернет
Программно-аппаратные средства платежных банковских систем
Программно-аппаратные средства системы дистанционного обучения
Система автоматизированого проектирования узлов вычислительной аппаратуры
Информационная система управления бизнесом в области объектов недвижимости
Автоматизированная система управления персоналом в крупной компании
Телекоммуникационный канал связи между филиалами банка
Телекоммуникационный канал связи между дилерами банка и валютной биржей
Широкополосный канал выхода в Интернет крупной международной компании
Межсетевой экран, обеспечивающий сегментацию локальной сети
Сервер учебного заведения, содержащий результаты тестирования студентов

Основные разделы проекта:

1. структурирование защищаемой информации;
2. моделирование возможных каналов утечки информации;
3. оценка степени угрозы защищаемой информации;
4. разработка мероприятий по защите информации на данном объекте;
5. выбор технических средств защиты информации на данном объекте;
6. разработка схемы размещения технических средств на объекте;
7. оценка степени защищенности информации;
8. оптимизация проекта по стоимости защиты.

В качестве исходных данных студенты выбирают объект защиты в виде офиса фирмы, выделенного помещения, в котором осуществляется работа с конфиденциальной информацией, комнаты для переговоров и т.п., которые могут быть образами аналогичных объектов по месту работы студента или знакомы ему по учебной практике.

Примерный объем пояснительной записки: 25-30 стр.

Требования к оформлению отражены в СТО ВоГУ «Письменные работы. Требования к оформлению».

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. - Ре- жим 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. Басалова, Г. В. Основы криптографии [Электронный ресурс] курс лекций / Г. В. Басалова. - Москва: ИНТУИТ, 2011. - 253 с. - Режим доступа: http://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 [Электронный ресурс]: курс/ О. Р. Лапонина. - 2-е изд., исправ. - Москва: ИНТУИТ, 2016. - 462 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429094	ЭБС «Университетская библиотека онлайн»
10. 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»
11. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для вузов/ В. П. Мельников, С. А.	5

Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 3-е изд., стер. - Москва: Academia, 2008. - 330, [1] с. ил.	
12. Петренко, В. И. Теоретические основы защиты информации [Электрон- ный 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»
13. 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»
14. 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
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, [1] с.	5
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»
16. 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
17. Технологии защиты информации в компьютерных сетях [Электрон- ный 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 «Университетская библиотека онлайн»
18. 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
19. Цирлов, В. Л. Основы информационной безопасности: краткий курс: [учебник для вузов]/ В. Л. Цирлов. - Ростов-на-Дону: Феникс, 2008. - 253, [1] с.	5
20. 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, [1] с.	7
21. 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

22. 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", "Разра- ботка программно-информационных систем"/ сост. Е. Н. Давыдова. - Во- логда: ВоГУ, 2014. - 31 с.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book10/2014_davydova_za sh_i nf.pdf	10 ЭБ ВоГУ
23. Методы и средства защиты компьютерной информации: методические указания к 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.: ил. - Режим доступа: http://www.library.vstu.edu.ru/biblio/davydova/book7/2009_davydova_4.pd f	29 ЭБ ВоГУ
24. 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_sukonshiko v_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

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