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.

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки / специальность: 09.03.01 Информатика и вычислительная техника

Направленность (профиль / специализация): Для всех профилей

Квалификация выпускника: бакалавр

Форма обучения: **Очная**

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

Кафедра: **автоматики и вычислительной техники**

Вологда

2026 г.

Составитель рабочей программы

заведующий кафедры, ктн, доцент / Суконщиков А.А. /

(должность, уч.степень, звание) *(Ф. И. О.)*

Рабочая программа дисциплины **КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ** 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 рассмотрена 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./

СОГЛАСОВАНО:

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

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины являются
1. Изучение методов, средств по обеспечению комплексной защиты информации.
2. Формирование навыков применения методов защиты от несанкционированного доступа.
3. Формирование навыков проведения экспериментальных исследований и обработки их результаты исходя из поставленных целей.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ УЧЕБНОГО ПЛАНА

Дисциплина относится к _ дисциплинам обязательной части _блока Б1 модулю профильной направленности.

Требования к предварительной подготовке обучающегося: математические основы теории систем, моделирование систем управления; основные понятия и аксиомы информатики, методы, устройство ЭВМ и основные методы и приемы работы с персональным компьютером.

Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее: 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 программного обеспечения
ПК-1.3. Формирует сборку модулей и компонент программного обеспечения
ПК-5. Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы
ПК-5.1. Изучает методы и способы по управлению работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы
ПК-5.2. Выполняет работы по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы
ПК-5.3. Управляет работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы

В результате освоения дисциплины обучающийся должен:

знать:

- основные методы и инструменты разработки комплексной защиты данных.

уметь:

- применять методы и инструменты комплексной защиты данных,
- обрабатывать и интерпретировать результаты исследований,
- описывать выполнение научных исследований;

владеть/быть в состоянии продемонстрировать:

- навыками использования операционных систем, сетевых технологий, применения языков и методов формальных спецификаций для комплексной защиты данных,
- методами комплексной защиты данных для решения профессиональных и социально-экономических задач в своей области деятельности владением.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

Общая трудоемкость дисциплины составляет _4_ ЗЕТ (__144_ 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.				
8/4	4	144	24	36	36	21	27	КР	Экзамен

№	Наименование разделов и тем/ вид занятия	Семестр/ сессия/ курс	Кол-во часов	Индикаторы достижения компетенций	Форма текущего контроля
1	Тема 1. Основные положения	8/4		ПК-1, 5, ОПК-3	
	Лекция 1. Классификация объектов защиты и угроз. Анализ угроз информационной безопасности. Основные методы реализации угроз.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 2. Основные принципы обеспечения информационной безопасности. Причины и каналы утечки информации.	8/4	2	ПК-1, 5, ОПК-3	
	Лабораторная работа 1. Изучение среды Cisco Packet Traser. Исследование защищенности элементов сети.	8/4	4	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 1. Определение угроз для конкретной организации.	8/4	4	ПК-1, 5, ОПК-3	Защита отчета
	Самостоятельная работа	8/4	4	ПК-1, 5, ОПК-3	
2	Тема 2. Построение Виртуальных локальных сетей (VLAN).	8/4		ПК-1, 5, ОПК-3	
	Лекция 1. Типы VLAN. VLAN на основе стандарта IEEE 802.1 Q.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 2. Статические и динамические VLAN .	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 3. VLAN на основе протоколов и	8/4	2	ПК-1, 5, ОПК-3	

	ассиметричные VLAN.			ПК-1, 5, ОПК-3	
	Лабораторная работа 1. Построение VLAN на различных сетях.	8/4	4*	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 1. Разработка методов защиты от НСД во внутренней сети.	8/4	4	ПК-1, 5, ОПК-3	Защита отчета
	Лабораторная работа 2. Построение статических и динамических VLAN на различных сетях.	8/4	4*	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 2. Разработка списков доступа во внутренней сети.	8/4	4	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 3. Разработка защиты сети на основе Q-in-Q.	8/4	4	ПК-1, 5, ОПК-3	Защита отчета
	Самостоятельная работа	8/4	5	ПК-1, 5, ОПК-3	
3	Тема 3. Функции обеспечения безопасности.	8/4		ПК-1, 5, ОПК-3	
	Лекция 1 Системы управления доступом ACL. Профили доступа и правила.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 2. Функции контроля за подключением к коммутатору.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 3. Аутентификация пользователей по IEEE 802.1X.	8/4	2	ПК-1, 5, ОПК-3	
	Лабораторная работа 1. Настройка ACL на коммутаторах. Построение профилей.	8/4	6	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 1. Построение на основе IEEE 802.1X защищенной внутренней сети.	8/4	4*	ПК-1, 5, ОПК-3	Защита отчета
	Самостоятельная работа	8/4	5	ПК-1, 5, ОПК-3	
4	Тема 4. Защита инфраструктуры маршрутизации.	8/4		ПК-1, 5, ОПК-3	
	Лекция 1 Общие сведения о протоколах маршрутизации. Угрозы для маршрутизации.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 2 Построение защищенной маршрутизируемой сети.	8/4	2	ПК-1, 5, ОПК-3	
	Лабораторная работа 1. Разработка защиты для маршрутизаторов.	8/4	6	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 1. Разработка маршрутизирующей сети.	8/4	4*	ПК-1, 5, ОПК-3	Защита отчета
	Самостоятельная работа	8/4	5	ПК-1, 5, ОПК-3	
5	Тема 5. Защита периметра сети	8/4		ПК-1, 5, ОПК-3	
	Лекция 1 Общие сведения о МСЭ. Возможные атаки на МСЭ.	8/4	2	ПК-1, 5, ОПК-3	
	Лекция 2 Построение защищенной сети от НСД.	8/4	4	ПК-1, 5, ОПК-3	
	Лабораторная работа 1. Построение защищенного МСЭ.	8/4	6*	ПК-1, 5, ОПК-3	Защита отчета
	Лабораторная работа 2. Защита беспроводной сети.	8/4	6*	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 1. Разработка комплексной защиты сети организации.	8/4	6*	ПК-1, 5, ОПК-3	Защита отчета
	Практическая работа 2. Моделирование разработанной комплексной защиты сети организации.	8/4	6*	ПК-1, 5, ОПК-3	Защита отчета
	Самостоятельная работа	8/4	2	ПК-1, 5, ОПК-3	
	ИТОГО	8/4	144		экзамен

*- занятия практической подготовки

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 экзамена могут включать:

- тесты, проводимые в письменной или электронной форме.

1. Пояснить рекомендации по настройке механизмов защиты виртуальных ЛВС.
2. Реализоватьв ЛВС атаку типа «VLAN hopping» при настройке различных собственных VLAN на транковых портах, соединяющих коммутаторы.
3. Настроить распространение базы данных VLAN через протокол VTP в соответствии с рекомендуемыми параметрами.
4. Настроить маршрутизацию VLAN на коммутаторе уровня ядра-распределения ЛВС.
5. Пояснить различия в работе между механизмами BPDU Guard, BPDU Filter и Root Guard.
6. Описать области применения и назначение каждого из этих механизмов защиты.
7. Пояснить выбор портов активации механизма Root Guard на коммутаторах уровня ядра-распределения филиала.
8. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MAC-адресов.
9. Объяснить рекомендацию задания максимального количества MAC-адресов на порту коммутатора с динамическим методом формирования списка из двух или трёх разрешенных MAC-адресов.
10. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

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 дальнейшем развитии навыков, опыта и знаний в области построения комплексной защиты информации с использованием рассмотренных на лекциях методов и технологий. Задание на курсовую работу состоит в разработке комплексной защиты корпоративной сети для различных организаций, разного количества машин, филиалов и потоков информации, более подробно информация приводится в методичке по курсовой работе.

Пояснительная записка должна адекватно отображать результаты основных этапов разработки комплексной защиты информации и содержать следующие этапы:

Введение (Актуальность внедрения комплексной защиты информации на данном предприятии)

1. Определение информационных потоков на предприятии , которые могут быть между отделами.
2. На основе данного раздела разработать структурную схему корпоративной сети.
3. Выбрать активное и пассивное оборудование сети.
4. Разработать защиту коммутаторов от несанкционированного доступа.
5. Разработать защиту маршрутизаторов от несанкционированного доступа.
6. Разработать схему VLAN.
7. Разработать защиту МСЭ от несанкционированного доступа.

8. Разработать защиту передачи данных к филиалу от несанкционированного доступа.
9. Составить списки доступа к серверам
10. Разработать структурную схему защищенной корпоративной сети и проанализировать полученные результаты.
11. Составить смету разработки проекта сети.
12. Составить выводы по разработке проекта.
13. Список используемых источников.

Примерный объем пояснительной записки: 25 стр., шрифт 12, интервал 1,5.
Примерный объем графической части: 5 листов формата А4

По дисциплине «Комплексная защита информации» студенты выполняют курсовую работу, которая состоит в разработке проекта защищенной корпоративной сети предприятия. Разработка состоит из нескольких подразделов, которые необходимо выполнить последовательно. Каждый студент выполняет свой вариант, который будет определяться последовательным номером студента в списке группы. Во всех вариантах заданий

предусматривается наличие филиалов, один из них в другом городе, другой в этом же, для обоих необходимо обеспечить удаленный доступ к корпоративной сети. Кроме того каждый вариант должен учитывать выход в Интернет, организацию почтового сервера, Веб - сервера, прокси - сервера, серверов баз данных, файл-серверов (PDC,BDC) и серверов для других сетевых приложений.

Варианты заданий по разработке защищенной корпоративной сети в следующих организациях. Номер варианта соответствует номеру студента в списке группы:

1 Информационная система для автоматизации организационно- распорядительного документооборота производственного предприятия.
2 Информационная система для автоматизации документооборота оперативного управления производственного предприятия.
3 Информационная система для автоматизации документооборота подсистемы сбыта производственного предприятия.
4 Информационная система для организационно- распорядительного документооборота учреждения
5 Информационная система для факультета университета
6 Информационная система для кафедры университета
7 Информационная система для торгового предприятия
8 Информационная система для авиапредприятия
9 Информационная система для лечебного учреждения (больницы)
10 Информационная система для лечебного учреждения (поликлиники)
11 Информационная система для банка
12 Информационная система для культурно-спортивного центра
13 Информационная система для издательства с филиалами в других городах
14 Информационная система для автотранспортного предприятия
15 Информационная система для предприятия связи
16 Информационная система для железнодорожного вокзала
17 Информационная система для школы (колледжа, гимназии)
18 Информационная система для выставочного центра
19 Информационная система для центра службы занятости
20 Информационная система для акционерного общества, имеющего филиалы
21 Информационная система для небольшой финансовой компании
22 Информационная система для небольшой инвестиционной фирмы
23 Информационная система для архитектурной организации
24 Информационная система для машиностроительного предприятия
25 Информационная система для строительного треста
26 Информационная система для гостиницы
27 Информационная система для милиции

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. Девянин, П. Н. Модели безопасности компьютерных систем: учебное пособие для вузов/ П. Н. Девянин. - Москва: Academia, 2005. - 143 с. . - (Высшее профессиональное образование. Информационная безопасность)	21
2. 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. . - (Высшее профессиональное образование. Информатика и вычислительная техника)	20
3. Методы и средства защиты компьютерной информации. Разработка системы защиты вычислительной системы: методические указания к практической работе № 3: ЭЭФ, ЗДО: специальности: 220201, 230101/ [сост. А. А. Суконщиков]. - Вологда: ВоГТУ, 2007. - 24 с.: ил. . - . - 10.80 URL: http://library.vogu35.ru/biblio/sukonshikov/book3/2007_sukonshikov_zash_pr3.pdf	39 ЭБ ВоГУ
4. 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. . - . - 38.53 URL: http://library.vogu35.ru/biblio/sukonshikov/book1/2008_sukonshikov_sash_inf.pdf	40 ЭБ ВоГУ
5. Нестеров Сергей Александрович Информационная безопасность: Учебник и практикум Для СПО/ Нестеров С. А. - Электрон. дан. - Москва: Издательство Юрайт, 2019. - 321 . - Режим доступа: https://www.biblio-online.ru. - ISBN 978-5-534-07979-1: 769.00 URL: https://www.biblio-online.ru/bcode/442312	ЭБС "Юрайт"
5 Внуков Андрей Анатольевич Основы информационной безопасности: защита информации : Учебное пособие Для СПО/ Внуков А. А. - 2-е изд.; испр. и доп. - Электрон. дан. - Москва: Издательство Юрайт, 2019. - 240 . - Режим доступа: https://www.biblio-online.ru. - ISBN 978-5-534-10711-1: 489.00 URL: https://www.biblio-online.ru/bcode/431332	ЭБС "Юрайт"

6.2. Информационное обеспечение

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информа-тизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с. URL: https://books.ifmo.ru/file/pdf/2006.pdf
2. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. -264 с : ил. URL: https://www.elec.ru/library/nauchnaya-i-tehnicheskaya-literatura/kompleksnaya-zashita-informacii/
3. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с. https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
4. Доступ к учебно-методическому комплексу кафедры АВТ URL: http://atpp.vstu.edu.ru/umk/
5. Доступ к учебно-методическому порталу ВоГУ. URL: https://do.vogu35.ru/

6.3 Программное обеспечение

Windows, LibreOffice, CiscoPacket Traser

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ / МОДУЛЯ

№№ п/п	Перечень основного оборудования
1.	*Персональный компьютер*
2.	*Проектор (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 _____ 202_ 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