

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 17.10.2025 15:06:46
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e70bf83b057

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет

информационных технологий и автоматизации
производственных процессов

Кафедра

интеллектуальных систем и информационной
безопасности



УТВЕРЖДАЮ

И.о. проректора по
учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства защиты информации в компьютерных системах

(наименование дисциплины)

09.04.01 Информатика и вычислительная техника

(код, наименование специальности)

Искусственный интеллект и цифровые двойники предприятий

(магистерская программа)

Квалификация

магистр

(бакалавр/специалист/магистр)

Форма обучения

очная

(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Методы и средства защиты информации в компьютерных системах» является изучение основных теоретических знаний, практических навыков в области методов и принципов построения и алгоритмов функционирования защиты информации при проектировании и использовании компьютерных систем.

Задачи изучения дисциплины:

- приобретение студентами знаний о методах защиты информации в компьютерных системах;
- приобретение практических навыков использования полученных знания при осуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Дисциплина направлена на формирование общепрофессиональной компетенции (ОПК-7) компетенции выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в часть БЛОКА 1, формируемой участниками образовательных отношений дисциплин «Дисциплины (модули)» подготовки студентов по специальности 09.04.01 «Информатика и вычислительная техника» («Искусственный интеллект и цифровые двойники предприятий»).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Защита информации», «Операционные системы», изученных обучающимися при прохождении подготовки по программе бакалавриата (специалитета).

Является основой для изучения следующих дисциплин: «Технологии администрирования и управления в компьютерных системах и сетях», «Проектирование встраиваемых компьютерных систем».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения общепрофессиональных задач деятельности, связанных с информационной безопасностью.

Курс является фундаментом для ориентации студентов в сфере защиты информации в компьютерных системах.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 ак.ч. Программой дисциплины предусмотрены лекционные (36 ч.), лабораторные (36 ч.) занятия и самостоятельная работа студента (108 ч.).

Дисциплина изучается на 1 курсе в 1 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Методы и средства защиты информации в компьютерных системах» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен осуществлять эффективное управление разработкой программных средств и проектов	ОПК-7	ОПК-7.1. Применяет методы и средства разработки программного обеспечения, методы управления проектами разработки программного обеспечения, способы организации проектных данных, нормативно-технические документы (стандарты и регламенты) по разработке программных средств и проектов

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единиц, 180 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		1
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	108	108
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	10	10
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к экзамену (диф.зачету)	35	35
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	180	180
з.е.	5	5

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 8 тем:

- тема 1 (Угрозы информации в компьютерных сетях);
- тема 2 (Способы обнаружения и уязвимостей и причины их возникновения);
- тема 3 (Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях);
- тема 4 (Протоколы аутентификации при удаленном доступе);
- тема 5 (Средства и методы обеспечения целостности и конфиденциальности);
- тема 6 (Средства защиты локальных сетей при подключении к Интернет);
- тема 7 (Обнаружение сетевых атак);
- тема 8 (Защита виртуальных частных сетей и беспроводных сетей).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	<i>Угрозы информации в компьютерных сетях</i>	Источники угроз. Способы классификация угроз. Причины возникновения угроз.	4	—	—	-	-
2	<i>Способы обнаружения и уязвимостей и причины их возникновения</i>	Сканеры портов и сканеры уязвимостей. Анализ алгоритмов программ и журналов работы программ с целью выявления уязвимостей. Ошибки программирования и администрирования, приводящие к появлению уязвимостей.	4	—	—	Хеш-функции	6
3	<i>Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях</i>	Электронный замок «Соболь». ПАК «SecretNet». ПАК «VipNet».	4	—	—	Комбинированные шифры	6
4	<i>Протоколы аутентификации при удаленном доступе</i>	Основы построения парольных систем. Идентификация и аутентификация. Классификация парольных систем по методам аутентификации. Угрозы парольным системам.	4	—	—	Шифрование с открытым ключом	6

Продолжение таблицы 3

1	2	3	4	5	6	7	8
5	<i>Средства и методы обеспечения целостности и конфиденциальности</i>	Электронные подписи. Криптографические средства защиты информации. Стеганография	4	—	-	Протоколы контроля целостности	6
6	<i>Средства защиты локальных сетей при подключении к Интернет</i>	Топологии сетей и маршрутизация. Использование межсетевых экранов (firewall). Системы обнаружения вторжений (IDS).	4	—	-	Протоколы электронной цифровой подписи	6
7	<i>Обнаружение сетевых атак</i>	Системы обнаружения вторжений (IDS). HoneyPot и HoneyNet. Использование снифферов.	4	-	-	Протоколы аутентификации и идентификации	6
8	<i>Защита виртуальных частных сетей и беспроводных сетей</i>	Принципы построения виртуальных частных сетей (VPN). Используемые протоколы. Законодательное регулирование использования беспроводных сетей. Угрозы в беспроводных сетях. Защита от атак «отказ в обслуживании». Защита от снифферов. Защита систем дистанционного банковского обслуживания.	8	-	-	-	-
Всего аудиторных часов			36	-	-	36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-7	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

- реферат (индивидуальное задание) – 20 баллов;
- лабораторные работы – всего 80 баллов.

Экзаменационная оценка проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Методы и средства защиты информации в компьютерных системах» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Отсутствует.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

- 1) Угрозы информации в компьютерных сетях.
- 2) Способы обнаружения и уязвимостей и причины их возникновения.
- 3) Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.
- 4) Протоколы аутентификации при удаленном доступе.
- 5) Средства и методы обеспечения целостности и конфиденциальности.
- 6) Средства защиты локальных сетей при подключении к Интернет.
- 7) Обнаружение сетевых атак.
- 8) Защита виртуальных частных сетей и беспроводных.
- 9) Цифровая валюта.
- 10) Даркнет и TOR.
- 11) Кибероружие и кибертерроризм.
- 12) Уязвимости компьютерных сетей.
- 13) Актуальные угрозы в настоящее время.
- 14) Система IDS.
- 15) Система IPS.
- 16) Система DPI.
- 17) Система HIDS.
- 18) Система SIEM.
- 19) Система DLP.
- 20) Система Firewall.
- 21) Система Antivirus.
- 22) Классификация вредоносного программного обеспечения.
- 23) Боевое программное обеспечение.
- 24) Классификация сетевых атак.
- 25) Доктрина информационной безопасности различных государств (www.twirpx.net).
- 26) Закрытые сегменты сети (военные, DarkNet, Air gap – воздушный зазор).
- 27) Концепция электронного правительства.
- 28) Точки входа и другие уязвимости.

29) История проникновения одной компьютерной крысы (журнал Компьютер-Пресс).

30) Организация кибервойск в разных странах мира (журнал Военное обозрение и др.).

31) Доктрины, концепции защиты политики безопасности компьютерных систем и сетей.

32) История заражения первым компьютерным червем Морриса (журнал Компьютер-Пресс) и план реагирования по его действия.

33) Планы реагирования на инциденты компьютерных угроз.

34) Форензика (расследование компьютерных преступлений).

35) Электронные деньги.

36) Аспекты защиты в промышленных сетях, WEB 3.0, IoT и др

37) Взлом пароля.

38) Сканирование сети.

39) Подмена пакетов в локальной сети (IP-spoofing) и перехват паролей.

40) Проведение DDOS атаки.

41) Подавление DHCP серверов.

42) Взлом и защита WiFi сетей.

43) Настройка фильтров firewall.

44) Настройка таблиц сетевых подключений маршрутизаторов.

45) Атаки с помощью botnet и противодействие им.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 Угрозы информации в компьютерных сетях

1) Приведите основные понятия защиты информации и информационной безопасности.

2) Дайте классификацию угроз информационной безопасности.

3) Приведите непосредственные виды угроз для компьютерных систем: угроза нарушения конфиденциальности, угроза нарушения целостности информации, угроза нарушения работоспособности. Угроза раскрытия параметров компьютерной системы.

4) Чем информационная безопасность отличается от кибербезопасности?

5) Каковы элементы кибербезопасности?

Тема 2 Способы обнаружения и уязвимостей и причины их возникновения

1) Как выявить уязвимости в компьютерных сетях?

2) Как защититься от уязвимостей?

3) Чем различаются уязвимость, эксплойт и атака?

4) Какие бывают уязвимости?

5) Как разработчики обнаруживают уязвимости?

Тема 3 Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях

1) Дайте определение понятию – информационная безопасность. Покажите особенности информационной безопасности в сфере компьютерных сетевых технологий. Дайте характеристики протокола https, криптопротоколов SSL, TLS.

2) Покажите принципы защита программ и данных с помощью электронных ключей. Опишите ключи на базе перепрограммируемой постоянной памяти. Опишите ключи на базе заказных чипов. Опишите ключи на базе микропроцессоров. Приведите примеры реализации ключей.

3) Опишите назначение, алгоритмы работы и использования смарт-карт и USB-ключей для аутентификации пользователей.

4) Укажите назначение ПО VipNet CUSTOM, ViPNet Office Firewall, ViPNet и Personal Firewall. Приведите их характеристики, общее и различие.

5) Охарактеризуйте использование программно-аппаратных средств для защиты ПО. Опишите работу аппаратных ключей защиты серии HASP.

6) Опишите аппаратные ключи защиты RuToken.

7) Опишите аппаратные ключи защиты eToken.

Тема 4 Протоколы аутентификации при удаленном доступе

1) Приведите определение понятия «факторы аутентификации».

2) Укажите протоколы строгой аутентификации на основе симметричных алгоритмов шифрования.

3) Укажите протоколы аутентификация с использованием ассиметричных алгоритмов шифрования.

4) Какие протоколы могут использоваться в аутентификации, основанной на использовании ЭЦП?

5) Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

Тема 5 Средства и методы обеспечения целостности и конфиденциальности

1) Приведите основные угрозы целостности.

2) Приведите основные угрозы конфиденциальности.

3) На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).

4) Приведите основные угрозы целостности. Дайте определение статической и динамической целостности.

5) Дайте понятие и определение электронной цифровой подписи. Приведите процедуры формирования цифровой подписи.

Тема 6 Средства защиты локальных сетей при подключении к Интернет

1) Чем отличается антивирус от EDR (Endpoint Detection & Response)?

2) Что такое DMZ?

3) Укажите назначение журнала событий, мониторинга и системы SIEM.

4) Приведите основные схемы сетевой защиты на базе межсетевых экранов.

5) Опишите применение межсетевых экранов для организации

виртуальных корпоративных сетей.

Тема 7 Обнаружение сетевых атак

- 1) Приведите классификация компьютерных атак и систем их обнаружения.
- 2) Опишите технологии построения систем обнаружения атак.
- 3) Опишите технологии обнаружения аномальной деятельности.
- 4) Опишите концепции обнаружения компьютерных угроз, а не атак.
- 5) Укажите методы защита от атак на web-сайты и web-браузеры.
- 6) Опишите сигнатурный метод защиты информации при сетевых атаках типа Teardrop.
- 7) Приведите прямые и косвенные признаки атак.

Тема 8 Защита виртуальных частных сетей и беспроводных сетей

- 1) Приведите методы и средства обеспечения информационной безопасности в беспроводных сетях типа IOT.
- 2) Какой функционал включают в себя межсетевые экраны следующего поколения (NGFW)?
- 3) Приведите характеристики маршрутизаторов и их функции безопасности.
- 4) Приведите характеристики коммутаторов и их функции безопасности.
- 5) Опишите межсетевые экраны. Приведите функции межсетевого экранирования.
- 6) Приведите виды и классификацию атак на сетевую инфраструктуру.
- 7) Приведите классификацию VPN.

6.5 Вопросы для подготовки к экзамену

- 1) Что представляет собой модель ISO/OSI?
- 2) Что представляет собой стек протоколов TCP/IP?
- 3) Какие типы сетевых атак на IP сети существуют?
- 4) Какие способы обеспечения информационной безопасности сетей существуют?
- 5) Какие стандарты обеспечения безопасности в беспроводных сетях существуют?
- 6) В чем разница между определениями и понятиями: идентификация, аутентификация, авторизация?
- 7) В чем состоит определение понятию аудит ИБ?
- 8) Какие существуют типы строгой аутентификации?
- 9) Какие способы биометрической аутентификации существуют?
- 10) Что понимается под словом «межсетевой экран» ?
- 11) Для каких целей служит межсетевой экран?
- 12) Какие схемы подключения МЭ применяются?
- 13) Какие классификации межсетевых экранов существуют?
- 14) Какие функции защиты прикладного шлюза существуют?
- 15) Как устроен программный вариант исполнения МЭ?
- 16) Как устроен программно-аппаратный вариант исполнения МЭ?
- 17) В чем состоит концепцию построения VPN?

- 18) Из каких компонентов состоит VPN?
- 19) Как классифицируются сети VPN по их назначению?
- 20) Что входит в структуру пакета для пересылки по туннелю PPTP?
- 21) Как устроена архитектура протокола L2TP?
- 22) Как устроен протокол SSL и установление сессии SSL?
- 23) Как работает схема установки соединения по протоколу SOCKS?
- 24) Как устроен протокол IPSec? Какая структура IP пакета?
- 25) Как устроен формат заголовка ESP?
- 26) Какие виды и классификации атак на сетевую инфраструктуру существуют?
- 27) Какие шифры замены применяют?
- 28) Какие шифры перестановки применяют?
- 29) Какие шифры гаммирования применяют?
- 30) Как работает схема режима шифрования DES-ECB?
- 31) Как работает тройной DES? Какая сфера применения различных режимов DES?
- 32) Как работает система шифрования ГОСТ 28147-89?
- 33) Как работает система шифрования AES?
- 34) Как работает шифрование с открытым ключом?
- 35) Как работает алгоритм шифрования RSA?
- 36) Как работает алгоритм шифрования Эль-Гамала?
- 37) Как устроен алгоритм шифрования на основе задачи об укладке ранца?
- 38) Как устроен алгоритм шифрования на основе эллиптических кривых?
- 39) Что представляют собой хэш-функции и какие характеристики они имеют?
- 40) Как работает хэш-функция MD5?
- 41) Какие протоколы обмена ключами существуют?
- 42) Какие протоколы аутентификации существуют (разновидности и краткая характеристика)?
- 43) Как устроен сервер аутентификации Kerberos?
- 44) Как работает алгоритм ЭЦП на базе алгоритма RSA?
- 45) Какие протоколы контроля целостности существуют (разновидности и краткая характеристика)?
- 46) Как работают алгоритмы электронных платежей (разновидности и краткая характеристика)?
- 47) Как работают протоколы контроля целостности (коды Хэмминга и ECC)?
- 48) Как работают алгоритмы цифровые деньги на базе "слепой" ЭЦП?
- 49) Какие существуют классификации сложности алгоритмов?
- 50) Как работают алгоритмы секретных кодовых систем?

6.6 Примерная тематика курсовых работ

Курсовые работы не предусмотрены.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «Форум» : Инфра – М., 2023. – 416 с. URL: <http://library.atu.kz/files/63376.pdf> (Дата обращения 20.08.2024).
2. Краковский, Ю.М. Методы защиты информации : учебное пособие для вузов / Ю.М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. URL: <https://e.lanbook.com/book/156401> (Дата обращения 20.08.2024).

Дополнительная литература

1. Сычев, Ю.Н. Защита информации и информационная безопасность: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю.Н. Сычев . — Москва : ИНФРА-М, 2023 . — 199 с. : ил. URL: https://library.bsuir.by/m/12_101945_1_157987.pdf (Дата обращения 20.08.2024).

Учебно-методические материалы и пособия

1. Закутный, А.С. Методы и средства защиты информации в компьютерных системах: лабораторный практикум [для студ. напр. подготовки 09.04.01 «Информатика и вычислительная техника» 6 курса всех форм обучения] / А.С. Закутный. — Алчевск : ГОУ ВО ЛНР «ДонГТИ», 2021. — 155 с. URL: <http://library.dstu.education/download.php?rec=123183>.

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education.— Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/>.— Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x>.— Текст : электронный.
4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red.— Текст : электронный.
5. Сайт кафедры ИСИБ <http://scs.dstu.education>.

Материально-техническое обеспечение представлено в таблице 6.

Таблица 6 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: <i>Мультимедийная аудитория. (60 посадочных мест), оборудованная специализированной (учебной) мебелью (скамья учебная – 20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран.</i> Аудитории для проведения лекций: <i>Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: ПК– 12 шт.; Доска – 1 шт.</i>	ауд. <u>207</u> корп. <u>4</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования рабочей программы дисциплины

Разработал

старший преподаватель кафедры
интеллектуальных систем
и информационной безопасности
(должность)


(подпись)

А.С. Закутный
(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

(должность)

(подпись)

(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности

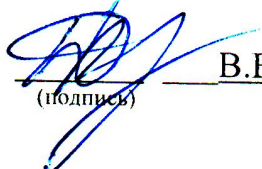

(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания
кафедры интеллектуальных систем и
информационной безопасности

от _____ 27.08.2024 г.

И.о. декана факультета информационных
технологий и автоматизации
производственных процессов


(подпись)

В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по направлению 09.04.01
«Информатика и вычислительная техника»
(искусственный интеллект и цифровые
двойники предприятий)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра


(подпись)

О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	