

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет математики и информационных технологий
Кафедра высшей математики и методики преподавания математики

УТВЕРЖДАЮ
проректор

_____ П. А. Машаров
«17» апреля 2025 г.
МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
И ЗАЩИТЫ ИНФОРМАЦИИ

Укрупненная группа направлений подготовки	44.00.00 Образование и педагогические науки
Программа высшего образования	Программа бакалавриата
Направление подготовки	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) образовательной программы	Математика и информатика
Квалификация	Бакалавр
Форма обучения	Очная

Рабочая программа может быть адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Донецк 2025

Рабочая программа дисциплины **«Основы информационной безопасности и защиты информации»** для обучающихся по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (Профиль: Математика и информатика), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), утвержденного приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 125 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2025 года.

Разработчик:

доцент кафедры высшей математики
и методики преподавания математики,

канд. пед. наук

Ю.В. Абраменкова

ассистент кафедры высшей математики
и методики преподавания математики

Д.А. Скворцова

Рабочая программа одобрена на заседании кафедры высшей математики и методики преподавания математики

Протокол от 10.04.2025 г. № 9

Заведующий кафедрой

Е.И. Скафа

СОГЛАСОВАНО:

Декан факультета математики и
информационных технологий

16.04.2025 г.

И. А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.

Протокол от 16.04.2025 г. № 3.

Председатель

Л. И. Селякова

Руководитель основной образовательной
программы, д-р пед. наук, проф.

16.04.2025 г.

Е.И. Скафа

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

дисциплины программы бакалавриата: Информатика, Алгоритмизация и программирование, Операционные системы и сети, Архитектура компьютера, Технологии искусственного интеллекта, Информационные системы и базы данных, Проектирование и разработка электронных образовательных ресурсов.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

История информатики, Компьютерная графика и обработка видео, Избранные разделы методики обучения информатике, Производственная практика: научно-исследовательская работа.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы (далее – ОП)	44.03.05 Педагогическое образование (с двумя профилями подготовки) (Профиль: Математика и информатика)
Шифр и название в соответствии с учебным планом	Б1.В.ОД.18 Основы информационной безопасности и защиты информации
Часть образовательной программы	Вариативная часть Безальтернативные дисциплины
Количество зачетных единиц / всего часов	3,5 / 126

В случае предъявления от обучающегося или его родителя (законного представителя) заявления на обучение по адаптированной образовательной программе высшего образования, подкрепленного заключением психолого-медико-педагогической комиссии (ПМПК) или медико-социальной экспертизы (МСЭ) с рекомендациями создания индивидуальной программы реабилитации и абилитации (ИПРА), данная рабочая программа может быть адаптирована с учетом индивидуальных особенностей здоровья обучающегося.

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	5	9	20	20	–	86	126	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Ознакомление студентов с основами обеспечения информационной безопасности и защиты информации, выработка представления о значимости обеспечения безопасности личности в информационном обществе

**4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ
ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ
И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

Компетенции	Индикаторы	Результаты обучения
ПК-4. Способен применять знание основных положений математической науки и информатики, основных положений истории развития математики и информатики, эволюции математических идей в профессиональной деятельности.	ПК-4.1. Демонстрирует способности использования инструментальных средств защиты информации	ПК-4.1.1. Знает сущность и понятие информационной безопасности, характеристику ее составляющих ПК-4.1.2. Знает особенности установки сетевых компонентов защиты информации. ПК-4.1.3. Знает современные средства и способы обеспечения информационной безопасности. ПК-4.1.4. Умеет настраивать сетевые службы защиты информационных систем
	ПК-4.2. Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности	ПК-4.2.1. Знает основные составляющие в области анализа систем информационной безопасности ПК-4.2.2. Владеет навыками применения современных технологий, применяемых в области информационной безопасности.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Информационная безопасность в системе национальной безопасности России	Основные понятия информационной безопасности. Место информационной безопасности в системе национальной безопасности РФ. Нормативная база информационной безопасности. Источники и содержание угроз в информационной сфере.
2. Методы защиты информации	Основные методы защиты информации. Направления защиты: правовая, организационная, техническая. Подходы к обеспечению информационной безопасности. Физическая, техническая и криптографическая защита информации. Идентификация и аутентификация пользователя. Управление доступом. Модели доступа. Контроль целостности. Защита от вредоносного программного обеспечения. Комплексный подход к защите информации. Системы обнаружения вторжений (СОВ). Требования к СОВ. Сравнительный анализ средств антивирусной защиты.
3. Информация как объект защиты	Свойства информации с точки зрения информационной безопасности. Виды информации в зависимости от категории доступа. Конфиденциальная информация. Жизненный цикл конфиденциальной информации в процессе ее создания, обработки, передачи. Классификация информации по видам тайн и степеням конфиденциальности. Технология электронной подписи. Защита информации в Интернете.

4. Классификация и общая характеристика программно-аппаратных средств защиты информации.	Классификация средств защиты информации. Средства криптографической защиты. Средства защиты от несанкционированного доступа. Средства защиты информации сетевого действия.
5. Защита компьютерной сети с помощью межсетевых экранов	Методы защиты в операционных системах. Сетевые технологии защиты. Вредоносные программы. Понятие брандмауэра. Компоненты брандмауэра. Политика межсетевого экранирования. Компьютерные преступления и наказания
6. Информационная безопасность в среде информационно-коммуникационных технологий.	Защита данных с помощью архивирования. Защита личной информации. Способы защиты личности. Технологии защиты от киберхулиганства и кибербуллинга.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 5, семестр – 9

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Информационная безопасность в системе национальной безопасности России	2	2		10	14
2. Методы защиты информации	2	2		10	14
3. Информация как объект защиты	2	2		10	14
4. Классификация и общая характеристика программно-аппаратных средств защиты информации.	4	4		18	26
5. Защита компьютерной сети с помощью межсетевых экранов	4	4		18	26
6. Информационная безопасность в среде информационно-коммуникационных технологий.	6	6		20	32
ИТОГО ЗА СЕМЕСТР	20	20	–	86	126

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Компьютерная система и защита информации.
2. Типичные требования к защите компьютерной системы.
3. Идентификация и аутентификация пользователей.
4. Ограничение доступа на вход в систему.
5. Разграничение доступа к информации.
6. Дискреционная модель разграничения доступа.
7. Мандатная модель разграничения доступа.
8. Регистрация событий аудит.
9. Криптографическая защита данных.
10. Классификация криптографических алгоритмов.
11. Контроль целостности данных.

12. Управление политикой безопасности.
13. Уничтожение остаточной информации.
14. Классификация программно-аппаратных средств защиты информации.
15. Состав комплексных систем защиты.
16. Системы криптозащиты и системы защиты от несанкционированного доступа.
17. Понятие межсетевого экрана. Политика межсетевого экранирования.
18. Компоненты межсетевого экрана.
19. Архитектура межсетевых экранов.
20. Основные функции VPN.
21. Туннелирование в VPN. Уровни защищенных каналов.
22. Защита данных на канальном уровне в VPN.
23. Применение МЭ на основе двудомного узла.
24. Применение МЭ на основе фильтрующего маршрутизатора. 24. Применение МЭ на основе экранирующего узла. 25. Применение технологии трансляции сетевых адресов.
25. Использование сканеров безопасности.
26. Анализ защищенности web-серверов.
27. Применение технологии терминального доступа.
28. Проектирование защиты IIS.
29. Создание концептуального плана защиты сетевой инфраструктуры
30. Проектирование логической защитной инфраструктуры
31. Проектирование физической защиты для инфраструктуры сети
32. Администрирование системы безопасности с помощью сетевых политик

7.2. Темы докладов (рефератов)

1. Компьютерные вирусы и другие вредоносные программы. Программы для защиты от вирусов.
2. Организация личного архива информации. Резервное копирование. Парольная защита архива.
3. Угрозы информационной безопасности при работе в глобальной сети и методы противодействия им. Правила безопасной аутентификации. Защита личной информации в Интернете.
4. Сетевой этикет: правила поведения в киберпространстве. Стратегии безопасного поведения в Интернете.
5. Основные понятия и принципы информационной безопасности.
6. Технологии аутентификации, авторизации и управления доступом.
7. Технологии безопасности на основе фильтрации и мониторинга трафика.
8. Атаки на транспортную инфраструктуру сети.
9. Безопасность программного кода и сетевых служб.
10. Организация виртуальных частных сетей.
11. Обеспечение безопасности межсетевого взаимодействия.
12. Удаленные сетевые атаки. Примеры атак и их классификация.
13. Технологии межсетевых экранов
14. Системы обнаружений атак и вторжений.
15. Виртуальные частные сети
16. Алгоритмы симметричного шифрования.
17. Алгоритмы симметричного шифрования AES.

7.3. Темы письменных работ (типы задач)

Примеры практических заданий:

1. Работа с браузером. Всплывающие окна, список сайтов, доступ к которым запрещен, очистка кэша браузера, файлы «cookie», плагин, работа с паролями в браузере.

2. Настройка прав доступа в операционной системе Windows. Создание учетных записей пользователя, Установление и восстановление паролей, настройки доступа личных папок.

3. Восстановление данных средствами операционной системы. Восстановление данных с помощью программы Recuva.

4. Защита данных с помощью архивирования. Защита личной информации при использовании сервисов Google.

5. Способы защиты личности.

6. Технологии защиты от киберхулиганства и кибербуллинга.

7.4. Образец содержания экзаменационного билета (при наличии экзамена по дисциплине)

БИЛЕТ №__

1. Классифицировать основные угрозы безопасности информации.

2. Источники угроз информационной безопасности и меры по их предотвращению.

3. Современные средства и способы обеспечения информационной безопасности.

Критерии оценивания экзаменационного билета

<i>Номер задания</i>	<i>Количество баллов</i>
Задание 1	30
Задание 2	30
Задание 3	40
<i>Всего</i>	<i>100</i>

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

Экзамен проводится для студентов с целью повышения их рейтинга, обобщения и систематизации знаний, полученных в результате изучения дисциплины. Время экзамена составляет 60 мин. Для студентов, которые будут сдавать экзамен, все набранные ими в течение семестра баллы обнуляются. Экзамен оценивается в 100 баллов. В него входят теоретические и практические задания.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже.

Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лабораторных занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Самостоятельная работа оценивается на основе предоставленных на проверку выполненных домашних заданий с учетом своевременности их предоставления и соответствия требованиям к их выполнению.

Количество баллов за контрольную работу вычисляется как сумма баллов за все входящие в её состав задания. Каждое задание оценивается исходя из максимально возможного количества баллов с учетом правильности выполнения задания, полноты приводимых обоснований.

8.1.Семестр 9

Номера разделов	Виды работ	Максимальное количество баллов
1	Организационно-учебная работа в аудитории	10
	Самостоятельная работа	20
	Лабораторные занятия	50
	Контрольная работа по теоретическому материалу	20
ИТОГО		100
Экзамен		100
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). Для проведения занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.705).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины могут применяться электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

10. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

10.1. Основная литература

1. Сухостат, В.В. Основы информационной безопасности : учебное пособие / В.В. Сухостат, И.Н. Васильева. – СПб. : Изд-во СПбГЭУ, 2019. – 103 с.
2. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.

3. Баранова, Е.К. Информационная безопасность и защита информации: Учеб. пособие / Е.К. Баранова, А.В. Бабаш. – 3-е изд, перераб. и доп. – Москва : РИОР : ИНФРА-М, 2016 – 322 с.

10.2. Дополнительная литература

4. Нестеров, С.А. Основы информационной безопасности : Учебное пособие. – 2-е изд., стер. – Санкт-Петербург : Издательство «Лань», 2020. – 324 с.

5. Ищейнов, В.Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. – Москва : ФОРУМ : ИНФРА-М, 2021. – 208 с.

6. Шаханова, М.В. Современные технологии информационной безопасности : учебно- методический комплекс. – Москва : Проспект, 2020. – 216 с.

11. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 31.03.2025). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.

2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 31.03.2025). – Режим доступа: для авторизов. пользователей. –Текст: электронный.

3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/> (дата обращения: 31.03.2025). – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 31.03.2025). – Режим доступа: издания Сетевой электронной библиотеки, для авторизов. пользователей. – Текст: электронный.

5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://urait.ru/library/svobodnyy-dostup/> (дата обращения: 31.03.2025). – Режим доступа: издания свободного доступа, для авторизов. пользователей. – Текст: электронный.

6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 31.03.2025). – Режим доступа: свободный. – Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 31.03.2025). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ:** раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 31.03.2025). – Режим доступа: свободный.

12. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).