

Министерство науки и высшего образования
Российской Федерации

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

Факультет дополнительного и профессионального образования
Кафедра инженерной и компьютерной педагогики



П.А. Машаров

« 29 » марта 2024 г.

МП

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Укрупненная группа направлений подготовки	44.00.00 - Образование и педагогические науки
Программа высшего образования	Программа бакалавриата
Направление подготовки	44.03.04 - Профессиональное обучение (по отраслям)
Профиль подготовки	Информатика и вычислительная техника
Квалификация	Бакалавр
Форма обучения	Очная, заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Информационная безопасность» для обучающихся по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям) (Профиль подготовки: Информатика и вычислительная техника), составлена на основании Федерального государственного образовательного стандарта высшего образования - бакалавриат по направлению подготовки 44.03.04 Профессиональное обучение (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 10 января 2018 г. № 8 (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 2024 года.

Разработчик:

ст. преподаватель кафедры инженерной и
компьютерной педагогики



М.П. Загорный

Рабочая программа одобрена на заседании кафедры инженерной и
компьютерной педагогики

Протокол от 26 . 03 .2024 г. № 10__



Заведующий кафедрой д-р пед. наук,
проф.

М.Г. Коляда

СОГЛАСОВАНО:

И.о. декана факультета дополнительного
и профессионального образования

28 . 03 .2024 г.



М.П. Загорный

Учебно-методическая комиссия факультета дополнительного и
профессионального образования.

Протокол от 27 . 03 .2024 г. № 7__.

Председатель



В.А. Тарасенко

Руководитель основной
профессиональной
образовательной программы,
д-р пед. наук, проф., зав. кафедрой ИКП
26 . 03 .2024 г.



М.Г. Коляда

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной. Для изучения данной учебной дисциплины необходимы знания и умения, формируемые параллельно идущими дисциплинами – Информационные технологии в образовании, Теоретические основы информатики, Основы программирования, Системы искусственного интеллекта, Системы управления базами данных.

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

Администрирование компьютерных систем и комплексов, Сетевые технологии и телекоммуникации, Производственная практика: научно-исследовательская работа, Производственная практика: преддипломная.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	44.03.04 Профессиональное обучение (по отраслям) (Профиль: Информатика и вычислительная техника)
Шифр и название в соответствии с учебным планом	Б1.В.ОД.2 Информационная безопасность
Часть образовательной программы	Вариативная часть (формируемая участниками образовательных отношений) Безальтернативные дисциплины
Количество зачетных единиц / всего часов	2,5 / 90

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	4	7	17	–	17	56	90	зачет
Заочная	5	9	4	–	2	84	90	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Информационная безопасность» – формирование теоретических знаний об основных принципах, методах и средствах обеспечения безопасности информационных технологий и защиты информации с использованием компьютерных средств в информационных системах. Задачами изучения дисциплины являются: формирование профессиональных навыков обеспечения безопасности информационных технологий и защиты информации; подготовка к деятельности, связанной с противодействием кибернетическим преступлениям.

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

4.1. Компетенции.

ПК-3. Способен осуществлять техническую поддержку создания, модификации и сопровождения информационных систем

4.2. Индикаторы компетенций

ПК-3.1. В результате изучения учебной дисциплины студент:

- выполняет анализ методов и средств передачи, хранения и обработки данных;
- управляет использованием информационных ресурсов при передаче конфиденциальной информации по техническим каналам;
- самостоятельно изучает и осваивает новые средства защиты информации;
- оценивает защищенность объектов информатизации;
- применяет методы защиты информации.

4.3. Результаты обучения

ПК-3.1.1. В результате изучения учебной дисциплины студент должен знать:

- средства и методы повышения безопасности информационных технологий;
- основные источники и носители информации разных видов;
- способы сбора, передачи, обработки и хранения информации;
- технические средства реализации информационных процессов;
- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по каналам, методы и средства контроля эффективности защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- основные законодательные и нормативные документы по защите информации;
- правовые основы деятельности подразделений защиты информации;
- основы криптографической и стеганографической защиты информации;
- основные демаскирующие признаки объектов защиты;
- возможности перехвата информации техническими средствами;
- активные и пассивные способы и средства сокрытия информации;
- способы и средства дезинформации;
- методы защиты информации и методы оценки их эффективности;

ПК-3.1.2. В результате изучения учебной дисциплины студент должен уметь:

- самостоятельно анализировать и оценивать факты, явления и события;
- раскрывать причинно-следственные связи между фактами, явлениями и событиями;
- пользоваться современной научно-технической литературой, нормативными и методическими материалами по обеспечению безопасности информационных технологий и защите информации;
- устанавливать связи между различными способами обработки информации;
- оценивать точность и достоверность полученной информации;
- описывать объекты защиты;

- организовывать защиту объекта активными и пассивными способами и техническими средствами;
- применять известные методы и средства защиты информации, проводить их сравнительный анализ;
- определять рациональные меры защиты на объектах и оценивать уровень и эффективность защиты;
- обеспечивать выбор оптимальных по условиям эксплуатации и экономичности средств защиты информации.

Компетенции	Индикаторы	Результаты обучения
ПК-3. Способен осуществлять техническую поддержку создания, модификации и сопровождения информационных систем	ПК-3.1. В результате изучения учебной дисциплины студент: выполняет анализ методов и средств передачи, хранения и обработки данных; управляет использованием информационных ресурсов при передаче конфиденциальной информации по техническим каналам; самостоятельно изучает и осваивает новые средства защиты информации; оценивает защищенность объектов информатизации; применяет методы защиты информации.	ПК-3.1.1. В результате изучения учебной дисциплины студент должен знать: средства и методы повышения безопасности информационных технологий; основные источники и носители информации разных видов; способы сбора, передачи, обработки и хранения информации; технические средства реализации информационных процессов; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по каналам, методы и средства контроля эффективности защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; основные законодательные и нормативные документы по защите информации; правовые основы деятельности подразделений защиты информации; основы криптографической и стеганографической защиты информации; основные демаскирующие признаки объектов защиты; возможности перехвата информации техническими средствами; активные и пассивные способы и средства сокрытия информации; способы и средства дезинформации; методы защиты информации и методы оценки их эффективности; ПК-3.1.2. В результате изучения учебной дисциплины студент должен уметь: самостоятельно анализировать и оценивать факты, явления и события; раскрывать причинно-следственные связи между фактами, явлениями и событиями;

		<p>пользоваться современной научно-технической литературой, нормативными и методическими материалами по обеспечению безопасности информационных технологий и защите информации;</p> <p>устанавливать связи между различными способами обработки информации;</p> <p>оценивать точность и достоверность полученной информации;</p> <p>описывать объекты защиты;</p> <p>организовывать защиту объекта активными и пассивными способами и техническими средствами;</p> <p>применять известные методы и средства защиты информации, проводить их сравнительный анализ;</p> <p>определять рациональные меры защиты на объектах и оценивать уровень и эффективность защиты;</p> <p>обеспечивать выбор оптимальных по условиям эксплуатации и экономичности средств защиты информации;</p>
--	--	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Тема 1. Безопасность информационных технологий.	Виды информации ограниченного доступа. Типы информационных угроз. Несанкционированный доступ к информации. Безопасность компьютерных систем: компьютерные вирусы и антивирусные программы, особенности удаленных угроз в компьютерных системах. Механизмы безопасности компьютерных сетей.
Тема 2. Защита информации.	Криптографические методы обеспечения защиты конфиденциальности, целостности и достоверности информации. Методы криптографического анализа. Оценка предельных мощностей взлома шифра. Защита информации в компьютерных системах с помощью стеганографических методов.
Тема 3. Компьютерные преступления.	Классификация технических каналов утечки информации. Методы добывания информации. Анализ компьютерных преступлений. Особенности раскрытия компьютерных преступлений. Правовые и организационные основы обеспечения информационной безопасности.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Форма обучения – очная, курс – 4 семестр – 7

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Безопасность информационных технологий.	6	–	6	18	30
Тема 2. Защита информации.	6	–	6	20	32
Тема 3. Компьютерные преступления.	5	–	5	18	28
ИТОГО ЗА КУРС	17	–	17	56	90

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

7.1. Контрольные вопросы

1. Виды информации ограниченного доступа
2. Модель информационной безопасности.
3. Структура и задачи службы безопасности.
4. Классификация нарушителей информационной безопасности.
5. Действия и события, нарушающие информационную безопасность.
6. Криптографические протоколы.
7. Симметричные шифры.
8. Поточные шифры.
9. Асимметричные шифры.
10. Хэш-функции.
11. Криптография открытого ключа.
12. Необратимые и односторонние функции.
13. Электронная цифровая подпись.
14. Защита информации в IP-сетях.
15. Система аутентификации Керберос.
16. Межсетевые экраны.
17. Криптоанализ симметричных шифров.
18. Криптоанализ асимметричных шифров.
19. Криптоанализ хэш-функций.
20. Криптоанализ по побочным каналам.
21. Атака по ключам.
22. Частотный анализ.
23. Сетевые черви
24. Скрипт-вирусы.
25. Троянские программы.
26. Особенности раскрытия компьютерных преступлений.
27. Методы незаконного проникновения.
28. Признаки компьютерных преступлений.
29. Методы и средства съема компьютерной информации в глобальных сетях.
30. Методы и средства съема компьютерной информации в ЛВС.

7.2. Темы докладов (рефератов)

1. Виды, источники и носители защищаемой информации.
2. Управление доступом как защита от несанкционированного доступа.
3. Типы информационных угроз.
4. Особенности удаленных угроз в компьютерных системах.
5. Механизмы безопасности компьютерных сетей.
6. Методы криптографического анализа.
7. Классификация технических каналов утечки информации.
8. Защита информации в компьютерных системах с помощью стеганографических методов.
9. Особенности раскрытия компьютерных преступлений.
10. Правовые и организационные основы обеспечения информационной безопасности.

Контрольная работа по проверке теоретических знаний – по всем темам, с использованием указанных выше контрольных вопросов.

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 лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Номера разделов	Виды работ	Максимальное количество баллов
1-3	Организационно-учебная работа в аудитории	40
	Самостоятельная работа	20
	Контрольная работа по теоретическому материалу	40
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. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в 3м корпусе ДонГУ (г. Донецк, ул. Щорса, 17). Для проведения практических 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 учебно-методических кабинетах 3-го корпуса (ауд. 108), материально-техническую базу учебной лаборатории «Охрана труда» кафедры инженерной и компьютерной педагогики.

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные в облачных хранилищах кафедры и ведущих преподавателей. При изучении дисциплины применяются 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.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Криптография и стеганография. Часть I Основы криптографии: учебно-методическое пособие для бакалавров направления подготовки 44.03.04 Профессиональное образование, профиль подготовки Информатика и вычислительная техника / ГОУ ВПО «ДОННУ»; сост. Бельков Д.В., Едемская Е.Н. – Донецк: ДонНУ, 2021. – 100 с.
2. Современные методы криптографии [Электронный ресурс] : учебное пособие / ГОУ ВПО "Донецкий национальный университет" ; сост.: Л. Н. Шкодина, А. И. Занько. - Донецк : ДонНУ, 2019.
3. Практический курс по современным методам криптографии [Электронный ресурс] : учебно-методическое пособие / ГОУ ВПО "Донецкий национальный университет" ; сост.: Л. Н. Шкодина, А. И. Занько. - 2-е изд. - Донецк : ДонНУ, 2019.
4. Скафа Е. И. Технологии эвристического обучения математике [Электронный ресурс] : учебное пособие / Е. И. Скафа, И. В. Гончарова, Ю. В. Абраменкова. – Донецк: ДонНУ, 2017. – Электронные данные (1 файл).

11.2. Дополнительная литература

5. Шкодина, Л. Н. Современные методы криптографии : учебное пособие / ГОУ ВПО "Донецкий национальный университет", Кафедра теории упругости и вычислительной математики имени академика А. С. Космодамианского ; составители: Л. Н. Шкодина, А. И. Занько. - Донецк : ДонНУ, 2019. - 113 с.
6. Методические указания к лабораторным работам по криптографии / [сост.: Л. Н. Шкодина, М. Н. Пачева, А. И. Занько] ; ГОУ ВПО "Донецкий национальный университет". - Донецк : ГОУ ВПО "ДонНУ", 2018. - 42 с..

12. 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: 01.09.2023). – 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: 01.09.2023). – Режим доступа: для авторизов. пользователей. –Текст: электронный.

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

4. Электронно-библиотечная система «Лань»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. ЭБС Юрайт: электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

6. Электронно-библиотечная система ДонГУ: сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – 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: 01.09.2023). – 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: 01.09.2023). – Режим доступа: свободный.

13. 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).