

Министерство науки и высшего образования
Российской Федерации

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

Факультет физико-технический
Кафедра радиофизики и инфокоммуникационных технологий



УТВЕРЖДАЮ

проректор

«29» марта 2024 г.

МП

П.А. Машаров

РАБОЧАЯ ПРОГРАММА КУРСОВОЙ РАБОТЫ

«МОДЕЛИ И МЕТОДЫ БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ОБМЕНА»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа бакалавриат
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Квалификация	Бакалавр
Форма обучения	очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа курсовой работы «**Модели и методы безопасного информационного обмена**» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (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:

Доцент
кафедры радиофизики
и инфокоммуникационных технологий

 В.И. Тимченко


Рабочая программа утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой

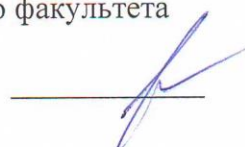
 В.В. Данилов

СОГЛАСОВАНО:

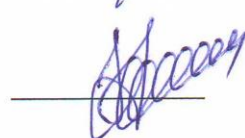
И.о. декана физико-технического факультета
28.03.2024 г.

 С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета
Протокол от 27.03.2024 г. № 2
Председатель

 В. Н. Котенко

Руководитель основной профессиональной образовательной программы
д-р тех. наук, проф.
26.03.2024 г.

 В.В. Данилов

1. МЕСТО КУРСОВОЙ РАБОТЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Основы теории сигналов и процессов, Информационные технологии, Архитектура компьютерных систем, История и философия науки.

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

Техническая защита информации, написание ВКР.

2. ОПИСАНИЕ КУРСОВОЙ РАБОТЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.В.ОД.17. Курсовая работа по дисциплине "Модели и методы безопасного информационного обмена"
Часть образовательной программы	Вариативная часть: выбор вуза
Количество зачетных единиц / всего часов	1,5 / 54

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, всего	3	5	-	-	-	54	54	зачет

3. ЦЕЛИ КУРСОВОЙ РАБОТЫ

Закрепление студентами знаний о современных методах выявления каналов изменения информации и несанкционированного доступа при ее передаче, хранении с помощью технических средств с учетом особенностей сигналов в инфокоммуникационных сетях и устройствах в их составе;

- математических, технических и организационных методов и алгоритмов, применяемых в системах хранения и обмена сигналами,

- ознакомления со средствами реализации мер обеспечения информационной безопасности в инфокоммуникационных сетях.

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

4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
УК-6 Способен управлять своим временем, выстраивать и реализовывать	УК-6.1 Способен управлять своим временем, выстраивать и	УК-6.1.1. Знает основы тайм-менеджмента, управления своим временем. Умеет организовывать самостоятельную работу,

траекторию саморазвития на основе принципов образования в течение всей жизни	реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	планировать этапы исследования, укладываться в назначенные сроки.
ОПК-8. Способен применять аппаратно-программные средства для безопасного информационного обмена	ОПК-8.1. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1.1. Знает нормативные и методические документы. Умеет применять аппаратно-программные средства для безопасного информационного обмена, работать с документацией.
ПК-2. Способен осуществлять мониторинг и управление функционированием систем связи, защищенностью от несанкционированного доступа.	ПК-2.1. Способен осуществлять мониторинг и управление функционированием средств связи сетей электросвязи и радиосвязи, защищенностью от несанкционированного доступа.	ПК-2.1.1. Способен использовать знания по применению методов поиска каналов утечки в профессиональной деятельности. Может выявлять и анализировать преимущества и недостатки вариантов предлагаемых решений, оценивает риски ПК-2.1.2. Может разработать методику получения и обработки сигналов. Может разработать методику определения характеристик контролируемых сигналов. Может проводить сбор исходных данных, необходимых для разработки систем защиты

5. ПРОГРАММА КУРСОВОЙ РАБОТЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Выбор темы курсовой работы	1. Выбор темы из предложенного списка или собственной темы.
2. Изучение источников и литературы по выбранной проблематике.	2.1. Анализ литературных источников. 2.2. Выписать наиболее значимые идеи и положения. 2.3. Наметить пути решения поставленных задач.
3. Составление плана исследования.	3.1. Выбор объекта и предмета исследования. 3.2. Постановка целей и задач 3.3. Обоснование методологии. 3.4. Составление плана исследования.
4. Написание курсовой работы согласно плану	4.1. Написание литобзора. 4.2. Проведение экспериментов, написание программы. 4.3. Описание выполнения практической части
5. Формулировка выводов по тематике исследования.	5.1. Формулировка выводов 5.2. Написание заключения. 5.3. Предоставление работы научному руководителю.

	5.4. Внесение правок по замечаниям научного руководителя.
6. Оформление текста курсовой работы согласно методическим рекомендациям	6.1. Оформление текста 6.2. Прохождение нормоконтроля. 6.3. Внесение правок по результатам нормоконтроля.
7. Предоставление курсовой на кафедру	7.1. Печать курсовой работы 7.2. Подпись у научного руководителя 7.3. Предоставление готовой курсовой на кафедру
8. Защита курсовой	8.1. Подготовка презентации и доклада. 8.2. Защита курсовой.

6. СТРУКТУРА И СОДЕРЖАНИЕ КУРСОВОЙ РАБОТЫ

6.1. Форма обучения – очная, курс – 2, семестр – 4

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
Выбор темы курсовой работы				1	1
Изучение источников и литературы по выбранной проблематике.				10	10
Составление плана исследования.				4	4
Написание курсовой работы согласно плану				30	30
Формулировка выводов по тематике исследования.				10	10
Оформление текста курсовой работы согласно методическим рекомендациям				3	3
Предоставление курсовой на кафедру				2	2
Защита курсовой				1	1
ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП				54	54
ИТОГО ПО КОМПОНЕНТУ ОПОП				54	54

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

7.1. Примерные темы для курсовой работы

1. Разработка модели защиты персональных данных пользователей онлайн-сервисов.
2. Исследование возможностей СЗИ для создания надёжных каналов удалённого доступа в различных операционных средах.
3. Применение алгоритмов машинного обучения к задаче обеспечения безопасности информационных систем.
4. Организация безопасного доступа в интернет с помощью СЗИ.
5. Анализ развития и возможностей использования сетей с нулевым доверием.
6. Разработка системы мониторинга и анализа защищённости сети на базе технологии Firewall/ IDS/IPS/ Vulnerability Assessment/ Security Policy Management/ VPN.
7. Разработка ПО для шифрования файлов с использованием алгоритма в различных режимах работы.
8. Разработка программного обеспечения по стандарту ГОСТ Р 56828.15–2016.
9. Анализ возможностей кибератак на нейросети в системах машинного зрения.

10. Разработка учебной документации для проведения инструментального аудита безопасности информации.

11. Разработка методики расследования инцидентов ИБ с помощью системы оркестровки, автоматизации и реагирования.

12. Разработка учебного практикума по изучению системы обнаружения вторжений на базе нейронной сети.

13. Исследование возможностей шлюза безопасности UserGate для обеспечения защиты информации, циркулирующей в корпоративной сети предприятия.

14. Система защиты информации автоматизированной картографической системы обработки геопространственных данных.

15. Разработка лабораторного практикума для изучения угроз ботнет-сетей и способов их предотвращения.

16. Разработка и внедрение системы мониторинга и анализа информационной безопасности предприятия.

17. Применение методов машинного обучения для прогнозирования и предотвращения кибератак.

18. Оценка и управление рисками информационной безопасности в организации.

19. Использование облачных технологий для повышения уровня безопасности данных.

20. Разработка и внедрение системы аутентификации пользователей на основе биометрических данных.

21. Анализ и сравнение различных подходов к обеспечению безопасности мобильных приложений.

22. Применение криптографических методов для защиты конфиденциальных данных.

23. Разработка и внедрение системы контроля доступа к информационным ресурсам предприятия.

24. Использование поведенческого анализа для выявления аномалий и угроз информационной безопасности.

25. Внедрение системы управления событиями безопасности (SIEM) на предприятии.

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
тема 1-17	Курсовая работа содержание	70
	Курсовая работа оформление	15
	Курсовая работа доклад	15
ИТОГО		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. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

10.1. Основная литература

1. Ерохин В. В. Безопасность информационных систем / В. В. Ерохин, Д. А. Погоньшева, И. Г. Степченко // Учебное пособие - М.: Флинта. Наука, 2015. - 184 с.
2. Белов Е.Б. Основы информационной безопасности: учеб, пособие для вузов / Е.Б. Белов, В.П. Лось. - М.: Горячая линия Телеком, 2006. - 544 с.
3. Занечников С.В. Информационная безопасность открытых систем. Т. I. Угрозы, уязвимости, атаки и подходы к защите / С.В. Занечников. И.Г. Милославская. А.И. Толстой. Д.В. Ушаков. - М.: Горячая Линия Телеком, 2006. - 536 с.
4. Крук Б.И. Телекоммуникационные системы и сети: учебное пособие. В 3 томах. / Б.И. Крук, Н.В. Нопантонопуло, В.Н. Шувалов. - Изд. 3-е, испр. и доп. - М.: Горячая линия - Телеком, 2003. - 647с.

10.2. Дополнительная литература

1. Креопалов В.В. Технические средства и методы защиты информации: учеб. - практ. пособие. -М.: Евразийский открытый институт, 2011,- 278 с

11. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Научная электронная библиотека elibrary.ru : информ.-аналит. портал / ООО Научная электронная библиотека. – Москва : ООО Науч. электрон. б-ка, сор. 2000–2022. – URL: <https://elibrary.ru> (дата обращения: 01.01.2023). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.
2. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2023). – Текст : электронный;
3. Учебники и другие книги по математике URL: <http://eqworld.ipmnet.ru/ru/library/mathematics.htm> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный
4. Интернет-библиотека Виталия Арнольда URL: <http://ilib.mcsme.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;
5. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;
6. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный.

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).