

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

П.А. Машаров

«29» марта 2024 г.

МП

РАБОЧАЯ ПРОГРАММА КУРСОВОЙ РАБОТЫ
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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 «**Основы информационной безопасности**» 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

 М.В. Бабичева

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:

Информатика, Информационные технологии, Технологии и методы программирования, Языки программирования, Теория информации, Архитектура компьютерных систем, Пакеты прикладных программ для обработки изображений, Модели и методы безопасного информационного обмена.

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

Web-программирование, Программно-аппаратные средства защиты информации, Методы и средства криптографической защиты информации.

Используются при написании выпускной квалификационной работы, Производственная практика: научно-исследовательская работа (обязательная). Производственная практика: преддипломная практика (обязательная).

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.Б.М3.18 Курсовая работа по дисциплине "Основы информационной безопасности"
Часть образовательной программы	Базовая(обязательная) часть
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	2	4	-	-	-	54	54	зачет

3. ЦЕЛИ КУРСОВОЙ РАБОТЫ

Закрепление знаний о понятиях национальной безопасности; видах безопасности; ИБ в системе национальной безопасности; основных понятий, общеметодологических принципов теории ИБ; анализе угроз ИБ, проблем информационной войны; государственной информационной политики; видах информации; методах и средствах обеспечения ИБ; методах нарушения конфиденциальности, целостности и доступности информации; причинах, видах, каналах утечки и искажения информации.

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 траекторию саморазвития на основе принципов образования в течение всей жизни.	УК-6.1. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.	УК-6.1.1. Знает основы тайм-менеджмента, управления своим временем. УК-6.1.2. Умеет организовывать самостоятельную работу, планировать этапы исследования, укладываться в назначенные сроки.
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.	ОПК-2.1 Умеет применять информационные технологии, в том числе языки программирования для решения задач профессиональной деятельности.	ОПК-2.1.1. Знает современные программные средства системного и прикладного назначения отечественного производства. ОПК-2.1.2. Умеет использовать современные программные средства системного и прикладного назначения для решения задач информационной безопасности.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	ОПК-5.1 Выбирает нормативные и правовые акты, методические документы и использует в профессиональной деятельности.	ОПК-5.1.1. Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности и умеет их применять для решения задач информационной безопасности.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной	ОПК-6.1 Способен применять современные технологии для защиты информации в соответствии с соответствующими нормативными документами.	ОПК-6.1.1. Знает методы обработки информации с использованием современных технических средств коммуникации и связи. ОПК-6.1.2. Умеет использовать современные информационно-коммуникационные технологии для решения задач информационной безопасности в соответствии с нормативными правовыми актами, нормативными и методическими документами

службы по техническому и экспортному контролю.		Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.	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. Умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности и использует их для решения профессиональных задач.

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. Радиозакладные устройства FM-диапазона.
2. Разработка макета BADUSB.
3. Разработка криптостойкого генератора псевдослучайной последовательности
4. Взлом хеша при помощи радужных таблиц. Программная реализация.
5. Реализация клиент-серверного приложения для удаленного доступа.
6. Применение кодировки base64 и реализация в демонстрационной программе.
7. Создание программы для демонстрации различных методов шифрования
8. Реализация перестановочных шифров и взлом их частотным анализом.
9. Инструменты сканирования портов. Расширенное сканирование.
10. Создание программного или аппаратного кейлоггера.
11. Создание стеганографического алгоритма.
12. Создание генератора безопасных паролей.
13. Встраивание информации в изображение методом LSB.
14. Алгоритм jpeg (демонстрационная программа).
15. Инструменты Kali Linux. Применение инструментов Kali Linux для решения задач по безопасности. Разработка лабораторной работы.
16. Создание программы для обфускации кода программы.
17. Разработка защищенной базы данных.
18. Экранирование пользовательского ввода. Разработка html страницы для безопасного ввода пароля.
19. Разработка программного модуля для взлома хешированного пароля методом брут-форса.
20. Применение эзотерических языков программирования для обфускации кода.
21. Протоколы шифрования wi-fi (программная реализация одного из протоколов.
22. Атака переполнение буфера (примеры атак с описанием).
23. Эксплойты. Metasploit Framework (использование + автоматический эксплоитнг).

24. Утилиты nslookup, whois, netcat, openssl, nmap. (провести разведку для атаки на сайт).
25. Коды Рида-Соломона (применение в QR кодах)
26. Исследование уязвимостей сайтов программой Acunetics.
27. Дорки для поиска уязвимых web- приложений. Провести поиск, эксплуатировать уязвимость.
28. Тестирование программ для восстановления данных на диске.
29. Граббер для чатов с Telegram API
30. Перехват http-запросов при помощи Burp Suite
31. Сканирование портов Nmap.
32. Создание tcp (http) сервера на сокетах (Python)
33. Разработка капчи (с проверкой).
34. Сравнительный анализ программ для взлома паролей.
35. Программа для демонстрации алгоритма Хаффмана.
36. Реализация схемы разделения секрета Шамира.

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. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов по специальности "Компьютерная безопасность и др. / П. Н. Девянин, О. О. Михальский, Д. И. Правиков и др. – М. : Радио и связь, 2000. - 192 с
2. Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. – 233 с.
3. Защита программного обеспечения / [Д. Гроувер, Р. Сатер, Дж. Фипс и др.] ; под ред. Д. Гроувера ; пер. с англ. В. Г. Потемкина и др. ; под ред. В. Г. Потемкина. – Москва : Мир, 1992. - 286 с.
4. Завгородний, В. И. Комплексная защита информации в компьютерных системах : Учеб. пособие для студентов вузов / В. И. Завгородний. – М. : Логос, 2001. - 264 с.

10.2. Дополнительная литература

5. Рассел, Ч. Microsoft Windows Server 2008 : справочник администратора / Ч. Рассел, Ш. Кроуфорд. – Москва : ЭКОМ Паблишерз, 2009. - 1321 с

6. Программно-аппаратные средства обеспечения информационной безопасности: Защита программ. и данных / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. - 169 с

7. Безопасность компьютерных сетей на основе Windows NT / В. С. Люцарев, К. В. Ермаков, Е. Б. Рудный, И. В. Ермаков. - М.: Рус. ред. TOO Channel Trading, 1998. – 304 с. + Электр. оптич. диск (CD-ROM).

11. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Интернет-Основы информационной безопасности . – URL: <http://www.intergu.ru/>

2. Сеть начинающих программистов. – URL: <http://www.it-n.ru/>

3. Классификация механизмов аутентификации пользователей и их обзор . – URL: <https://habr.com/ru/post/177551/>

4. SQL инъекции. Проверка, взлом, защита . – URL: <https://habr.com/ru/post/130826/>

5. XSS глазами злоумышленника. – URL: <https://habr.com/ru/post/66057/>

6. Stealthphone: Защита микрофона мобильного телефона от несанкционированного включения . – URL: <https://habr.com/ru/company/ancort/blog/160215/>

7. Основные параметры передатчиков и приемников . – URL: <https://radiokot.ru/start/analog/bugs/02/>

8. 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.

9. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2023). – Текст : электронный;

10. 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

11. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

12. 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. Яндекс Браузер (свободно распространяемое ПО)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения)
5. Kali Linux (свободно распространяемое ПО)
6. Stegsolve (свободно распространяемое ПО)