

Министерство науки и высшего образования  
Российской Федерации

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

Факультет математики и информационных технологий  
Кафедра прикладной механики и компьютерных технологий



П.А. Машаров

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ**

Укрупненная группа направлений  
подготовки  
Программа высшего образования  
Направление подготовки  
Магистерская программа  
Квалификация  
Форма обучения

09.00.00 Информатика и вычислительная  
техника  
Программа магистратуры  
09.04.04 Программная инженерия  
Программная инженерия  
Магистр  
Очная

Рабочая программа адаптирована для лиц  
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Компьютерная безопасность» для обучающихся по направлению подготовки 09.04.04 Программная инженерия (Магистерская программа: Программная инженерия), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 09.04.04 Программная инженерия, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 932 (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:  
доц. кафедры прикладной механики  
и компьютерных технологий,  
канд. физ.-мат. наук, доцент



Н.Н. Щепин

Рабочая программа одобрена на заседании кафедры прикладной механики и компьютерных технологий  
Протокол от 26.03.2024 г. № 14

Заведующий кафедрой



А.С. Гольцев

СОГЛАСОВАНО:

Декан факультета математики и  
информационных технологий  
28.03.2024 г.



И.А. Моисеенко

Учебно-методическая комиссия факультета математики и информационных технологий.  
Протокол от 27.03.2024 г. № 3.  
Председатель



Л. И. Селякова

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



А.С. Гольцев

## 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, Архитектура компьютеров, Информатика и программирование, Основы программной инженерии, Операционные системы, Компьютерные сети, Защита информации.

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

Производственная практика: научно-исследовательская работа, Производственная практика: технологическая (проектно-технологическая) практика, Производственная практика: преддипломная практика.

## 2. ОПИСАНИЕ ДИСЦИПЛИНЫ

### 2.1.Общая характеристика

| Наименование показателя                         | Значение показателя   |
|---|---|
| Название образовательной программы              | 09.04.04 Программная инженерия<br>(Магистерская программа: Программная инженерия) |
| Шифр и название в соответствии с учебным планом | Б1.Б.8 Компьютерная безопасность  |
| Часть образовательной программы                 | Вариативная часть: выбор вуза   |
| Количество зачетных единиц / всего часов        | 6 / 216   |

### 2.2.Распределение часов по формам и периодам обучения

| Форма обучения | курс | семестр | Общее количество часов |               |               |                         |       | Форма контроля |
|----------------|------|---------|------------------------|---------------|---------------|-------------------------|-------|----------------|
|                |      |         | лекци-онных            | лабора-торных | практи-ческих | самостоя-тельной работы | всего |                |
| Очная          | 1    | 2       | 34                     | 34            | 0             | 148                     | 216   | экзамен        |

## 3. ЦЕЛИ ДИСЦИПЛИНЫ

Цель - подготовка в области применения современных систем информационной безопасности и построения полномасштабной системы безопасности информационной инфраструктуры предприятия.

Задачи – изучение основных организационных и технических систем и средств защиты информации; принципов и методов противодействия несанкционированному доступу к информации; классификации систем и средств обеспечения информационной безопасности; знание базовых принципов функционирования различных систем и средств защиты информации.

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

### 4.1. Компетенции

ОПК-3. Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.

ПК-2. Способен модернизировать программное средство и его окружение.

ПК-3. Способен осуществлять контроль реализации программного средства (Профстандарт 06.003 – Архитектор программного обеспечения. ОТФ F).

ПК-7. Способен оценить требования к программному средству.

#### 4.2. Индикаторы компетенций

ОПК-3.1. Владеет организационными и техническими основами систем и средств защиты информации.

ОПК-3.2. Владеет базовыми принципами функционирования различных систем и средств защиты информации.

ПК-2.1. Владеет методами противодействия несанкционированному доступу к информации.

ПК-3.1. Владеет методами противодействия несанкционированному доступу к информации

ПК-7.1. Владеет навыками настройки групповых политик

#### 4.3. Результаты обучения

ОПК-3.1.1. Знает основные понятия защиты информационных систем.

ОПК-3.1.2. Знает общие требования к системам защиты информации.

ОПК-3.1.3. Знает классификацию систем защиты информации.

ОПК-3.2.1. Умеет выявлять возможные способы нарушения информационной безопасности при работе с автоматизированными системами обработки и хранения.

ОПК-3.2.2. Умеет применять нормативную базу обеспечения деятельности в области защиты информации

ОПК-3.2.3. Умеет осуществлять организационные мероприятия по обеспечению информационной безопасности

ПК-2.1.1. Знает основные методы противодействия несанкционированному доступу.

ПК-2.1.2. Умеет применять технические мероприятия по обеспечению информационной безопасности.

ПК-2.1.3. Знает основы технологии управления доступом и авторизации.

ПК-3.1.1. Знает основные методы противодействия несанкционированному доступу.

ПК-3.1.2. Умеет применять технические мероприятия по обеспечению информационной безопасности.

ПК-3.1.3. Знает основы технологии управления доступом и авторизации.

ПК-7.1.1. Знает классы групповых политик.

ПК-7.1.2. Знает основные параметры групповых политик.

ПК-7.1.3. Умеет настраивать групповые политики.

### 5. ПРОГРАММА ДИСЦИПЛИНЫ

| Название темы   | Краткое содержание темы (вопросы темы)   |
|---|--|
| Раздел 1.   |  |
| <b>Тема 1.</b> Основные понятия и принципы информационной безопасности. | Идентификация, аутентификация и авторизация. Модели информационной безопасности. Ущерб и риск. Управление рисками. Типы и примеры атак. Иерархия средств защиты от информационных угроз. |

|  |   |
|--|---|
|  | Принципы защиты информационной системы. Шифрование — базовая технология безопасности.   |
| <b>Тема 2.</b> Технологии аутентификации, авторизации и управления доступом.     | Технологии аутентификации. Технологии управления доступом и авторизации. Системы аутентификации и управления доступом операционных систем. Централизованные системы аутентификации и авторизации.   |
| <b>Тема 3.</b> Технологии безопасности на основе фильтрации мониторинга трафика* | Фильтрация. Файерволы. Прокси-серверы. Файерволы с функцией NAT. Программные файерволы хоста. Типовые архитектуры сетей, защищаемых файерволами. Мониторинг трафика. Анализаторы протоколов. Архитектура сети с защитой периметра и разделением внутренних зон. Аудит событий безопасности. |
| Раздел 2.  |   |
| <b>Тема 4.</b> Атаки на транспортную инфраструктуру сети                         | TCP-атаки. ICMP-атаки. UDP-атаки. IP-атаки. Сетевая разведка. Атаки на DNS. Безопасность маршрутизации на основе BGP. Технологии защищенного канала.  |
| <b>Тема 5.</b> Безопасность программного кода и сетевых служб*                   | Уязвимости программного кода и вредоносные программы. Безопасность веб-сервиса. Безопасность электронной почты. Облачные сервисы и их безопасность.   |
| <b>Тема 6.</b> Организация виртуальных частных сетей                             | Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.   |

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 6.1. Форма обучения – очная, курс – 1, семестр – 2

| Наименования разделов и тем  | Количество часов |        |        |     |       |
|--|------------------|--------|--------|-----|-------|
|  | Лекц.            | Лабор. | Практ. | СРС | Всего |
| Раздел 1.  | 18               | 18     | 0      | 73  | 109   |
| <b>Тема 1.</b> Основные понятия и принципы информационной безопасности.          | 4                |        | 0      | 25  | 29    |
| <b>Тема 2.</b> Технологии аутентификации, авторизации и управления доступом.     | 6                | 8      | 0      | 24  | 38    |
| <b>Тема 3.</b> Технологии безопасности на основе фильтрации мониторинга трафика* | 8                | 10     | 0      | 24  | 42    |
| Раздел 2.  | 16               | 16     | 0      | 75  | 107   |
| <b>Тема 4.</b> Атаки на транспортную инфраструктуру сети                         | 4                |        | 0      | 25  | 29    |
| <b>Тема 5.</b> Безопасность программного кода и сетевых служб*                   | 6                | 8      | 0      | 25  | 39    |
| <b>Тема 6.</b> Организация виртуальных частных сетей                             | 6                | 8      | 0      | 25  | 39    |
| ПО КОМПОНЕНТУ ОПОП   | 34               | 34     | 0      | 148 | 216   |

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

### 7.1. Контрольные вопросы

#### Раздел 1

1. Идентификация, аутентификация и авторизация.
2. Модели информационной безопасности.
3. Ущерб и риск.
4. Управление рисками.
5. Типы и примеры атак.
6. Иерархия средств защиты от информационных угроз.
7. Принципы защиты информационной системы.
8. Шифрование — базовая технология безопасности.
9. Технологии аутентификации.
10. Технологии управления доступом и авторизации.
11. Системы аутентификации и управления доступом операционных систем.
12. Централизованные системы аутентификации и авторизации.
13. Фильтрация.
14. Файерволы.
15. Прокси-серверы.
16. Файерволы с функцией NAT.
17. Программные файерволы хоста.
18. Типовые архитектуры сетей, защищаемых файерволами.
19. Мониторинг трафика.
20. Анализаторы протоколов.
21. Архитектура сети с защитой периметра и разделением внутренних зон.
22. Аудит событий безопасности.

#### Раздел 2

23. TCP-атаки.
24. ICMP-атаки.
25. UDP-атаки.
26. IP-атаки.
27. Сетевая разведка.
28. Атаки на DNS.
29. Безопасность маршрутизации на основе BGP.
30. Технологии защищенного канала.
31. Уязвимости программного кода и вредоносные программы.
32. Безопасность веб-сервиса.
33. Безопасность электронной почты.
34. Облачные сервисы и их безопасность.
35. Задачи, решаемые VPN.
36. Туннелирование в VPN.
37. Уровни защищенных каналов.
38. Защита данных на канальном уровне.

### 7.2. Темы докладов (рефератов)

- Основные понятия и принципы информационной безопасности.
- Технологии аутентификации, авторизации и управления доступом.
- Технологии безопасности на основе фильтрации и мониторинга трафика.
- Атаки на транспортную инфраструктуру сети.

- Безопасность программного кода и сетевых служб.
- Организация виртуальных частных сетей.
- Обеспечение безопасности межсетевого взаимодействия. Компьютерные вирусы.
- Удаленные сетевые атаки. Примеры атак и их классификация.
- Технологии межсетевых экранов
- Системы обнаружений атак и вторжений.
- Виртуальные частные сети
- Алгоритмы симметричного шифрования.
- Алгоритмы симметричного шифрования AES.

7.3. Темы письменных работ (типы задач)

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

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

**ФГБОУ ВО «ДОНЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Факультет математики и информационных технологий

Направление подготовки:

**09.04.04 Программная инженерия**

Магистерская программа:

**Программная инженерия**

Программа подготовки:

**академическая магистратура**

Семестр

**2**

Учебная дисциплина

**Компьютерная безопасность**

**БИЛЕТ №1**

1. Применение технологии трансляции сетевых адресов.
2. Использование сканеров безопасности.
3. Анализ защищенности web-серверов.

**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 заданий по лабораторным работам, активность во время проведения лекционных, практических и лабораторных занятий (участие в обсуждении текущего и пройденного материала и т.п.).

**8.1.Семестр 1**

| Номера разделов       | Виды работ                                     | Максимальное количество баллов |
|-----------------------|--|--------------------------------|
| 1-2                   | Организационно-учебная работа в аудитории      | 5                              |
|                       | Самостоятельная работа                         | 10                             |
|                       | Лабораторные работы                            | 25                             |
|                       | Контрольная работа по теоретическому материалу | 10                             |
| ИТОГО                 |  | 50                             |
| Экзамен               |  | 50                             |
| 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 зачет 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 Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6) и двенадцатом (г. Донецк, ул. Университетская, 24-а, УПВЦ). Для проведения лабораторных 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.505).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». 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. Современные сетевые технологии и компьютерная безопасность: учебное пособие / Сост.: Н.Н. Щепин, С.А. Прийменко, Р.Н. Нескороев. – Донецк: ДонНУ, 2019. – 158 с.
2. Компьютерная безопасность: учебно-методическое пособие / Сост.: Н.Н. Щепин. – Донецк: ДонНУ, 2019. – 84 с.
3. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Москва [и др.] : Питер, 2010. - 943 с.

### 11.2. Дополнительная литература

4. Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл ; [пер. с англ. А. Гребеньков]. - 5-е изд. - Санкт-Петербург [и др.] : Питер, 2012. - 955 с.
5. Олифер, В. Г. Сетевые операционные системы : [Учеб. пособие для студентов вузов по направлению подгот. дипломир. специалистов "Информатика и вычислительная техника] / В. Г. Олифер, Н. А. Олифер. - СПб. и др. : Питер, 2003. - 538 с.
6. Спортак, М. Компьютерные сети и сетевые технологии : Platinum Editions / М. Спортак, Ф. Ч. Паппас, Р. Пит и др. - М. : DiaSoft, 2005. - 720 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).