Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ КемГУ
Дата и время: 2025-04-23 00:00:00
471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кузбасский гуманитарно-педагогический институт

Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан
А. В. Фомина
«08» февраля 2024 г.

# Рабочая программа дисциплины

К.М.07.04 Информационная безопасность

Направление подготовки
09.03.01 Информатика и вычислительная техника

Направленность (профиль) подготовки
Автоматизированные системы обработки информации и управления

Программа бакалавриата

Квалификация выпускника
*бакалавр*

Форма обучения
*Очная*

Год набора 2024

Новокузнецк 2024

**Лист внесения изменений**

в РПД К.М.07.04 Информационная безопасность

*(код по учебному плану, название дисциплины)*

**Сведения об утверждении:**

утверждена Ученым советом факультета информатики, математики и экономики

протокол Ученого совета факультета № 7 от 08.02.2024 г.

для ОПОП 2024 год набора на 2024 / 2025 учебный год

по направлению подготовки 09.03.01 Информатика и вычислительная техника

направленность (профиль) Автоматизированные системы обработки информации и управления

Одобрена на заседании методической комиссии факультета информатики, математики и экономики

протокол методической комиссии факультета № 7 от 08.02.2024 г.

Одобрена на заседании обеспечивающей кафедры информатики и вычислительной техники им. В.К. Буторина

протокол № 6 от 25.01.2024 г. Зав. кафедрой А. В. Маркидонов

СОДЕРЖАНИЕ

1. Цель дисциплины ....4
Формируемые компетенции, индикаторы достижения компетенций, знания, умения, навыки ....4
Место дисциплины....5
2. Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации. ....5
3. Учебно-тематический план и содержание дисциплины. ....6
3.1. Учебно-тематический план....6
4. Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации....6
5. Материально-техническое, программное и учебно-методическое обеспечение дисциплины..7
5.1. Учебная литература....7
5.2. Материально-техническое и программное обеспечение дисциплины. ....8
5.3. Современные профессиональные базы данных и информационные справочные системы. 9
6. Иные сведения и (или) материалы. ....9
6.1. Примерные темы письменных учебных работ....9
6.2. Примерные вопросы и задания / задачи для промежуточной аттестации ....10

## 1. Цель дисциплины

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее ОПОП): ОПК-3.

**Формируемые компетенции, индикаторы достижения компетенций, знания, умения, навыки**

Таблица 1 - Индикаторы достижения компетенций, формируемые дисциплиной

| Код и название компетенции | Индикаторы достижения компетенции по ОПОП | Знания, умения, навыки (ЗУВ), формируемые дисциплиной |
|---|---|---|
| ОПК-3 | ОПК-3.5. Выявляет угрозы информационной безопасности;<br>ОПК-3.6. Анализирует и выбирает методы и средства обеспечения информационной безопасности в соответствии с заданием. | Знать:<br>– базовые понятия информационной безопасности;<br>– классификацию угроз уязвимостей;<br>– нормативно-правовую базу в области защиты информации;<br>– основные понятия и методы организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности;<br>– методики построения систем защиты информации.<br>Уметь:<br>– моделировать угрозы и уязвимости информационной безопасности;<br>– выделять источники информации, объекты защищаемой информации;<br>– формировать требования к построению безопасной системы;<br>– определять функциональные задачи и требования.<br>Владеть:<br>– методами организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности;<br>– методами и методиками построения систем защиты информации;<br>– программными продуктами для оценки риска информационной безопасности;<br>– программными средствами обеспечения информационной безопасности;<br>– протоколами аутентификации, распределения ключей, электронной подписи и финансовой криптографии. |

**Место дисциплины**

Дисциплина включена в модуль «Современные информационные технологии и информационные системы» ОПОП ВО, обязательная часть. Дисциплина осваивается на 3 курсе в 5 семестре.

## 2. Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 4 – Объем и трудоемкость дисциплины по видам учебных занятий

| Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах | Объём часов по формам обучения |
|---|---|
| | ОФО |
| 1 Общая трудоемкость дисциплины | 180 |
| 2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего) | 54 |
| Аудиторная работа (всего): | 54 |
| в том числе: | |
| лекции | 18 |
| практические занятия, семинары | 36 |
| практикумы | |
| лабораторные работы | |
| в интерактивной форме | |
| в электронной форме | |
| Внеаудиторная работа (всего): | |
| в том числе, индивидуальная работа обучающихся с преподавателем | |
| подготовка курсовой работы /контактная работа | |
| групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем) | |
| творческая работа (эссе) | |
| 3 Самостоятельная работа обучающихся (всего) | 90 |
| 4 Промежуточная аттестация обучающегося – экзамен – 5 семестр | 36 |

## 3. Учебно-тематический план и содержание дисциплины.

### 3.1. Учебно-тематический план

Таблица 3 - Учебно-тематический план очной формы обучения

| № п/п | Разделы и темы дисциплины по занятиям | Общая трудоёмкость *(всего час.)* | Трудоемкость занятий (час.) | | | Формы текущего контроля и промежуточной аттестации успеваемости |
|---|---|---|---|---|---|---|
| | | | Аудиторн. занятия | | СРС | |
| | | | лекц. | практ. | | |
| 1. | Введение в предмет. Угрозы информационной безопасности | 16 | 2 | 6 | 7 | Устный доклад; отчет по практической работе. |
| 2. | Основные понятия теории информационной безопасности | 16 | 3 | 6 | 7 | Устный доклад; Отчет по практической работе. |
| 3. | Программно-технические методы защиты | 25 | 3 | 6 | 16 | Устный доклад; Отчет по практической работе. |
| 4. | Криптографические методы защиты | 25 | 3 | 6 | 16 | Устный доклад; Отчет по практической работе. |
| 5. | Организационно правовые методы информационной безопасности | 18 | 3 | 8 | 7 | Устный доклад; Отчет по практической работе. |
| 6. | Роль стандартов в обеспечении информационной безопасности | 18 | 3 | 8 | 7 | Устный доклад; Отчет по практической работе. |
| 7. | Технологии построения защищенных систем | 27 | 3 | 8 | 16 | Устный доклад; Отчет по практической работе |
| 8. | Промежуточная аттестация -экзамен | 36 | | | | |
| **ИТОГО** | | **180** | **18** | **36** | **90** | **36** |

## 4. Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 4.

Таблица 4 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

| Учебная работа (виды) | Сумма баллов | Виды и результаты учебной работы | Оценка в аттестации | Баллы |
|---|---|---|---|---|
| Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий) | **60** | Лекционные занятия (конспект) | – посещение 1 лекционного занятия | 5 - 10 |
| | | Практические занятия | – посещение практического занятия и выполнение задания на 51-85%<br>– посещение практического занятия и выполнение задания на 85.1-100% | 10 - 20 |
| | | Отчет по практической работе | – задание выполнено в полном объеме, но имеются существенные неточности и недочеты, в оформлении работы есть нарушения;<br>– задание выполнено в полном объеме оформление соответствует требованиям, но есть недочеты в оформлении и общие небольшие замечания, не влияющие на качество работы<br>– задание выполнено в полном объеме, оформление на 100% соответствует требованиям | 16 - 30 |
| **Итого по текущей работе в семестре** | | | | **31 - 60** |
| Промежуточная аттестация (экзамен) | **40** | Теоретический вопрос 1 | **2 балла** (пороговое значение)<br>**10 баллов** (максимальное значение) | 5 - 10 |
| | | Теоретический вопрос 2 | **2 балла** (пороговое значение)<br>**10 баллов** (максимальное значение) | 5 - 10 |
| | | Практическое задание | | 10 – 20 |
| **Итого по промежуточной аттестации** | | | | **20 - 40** |
| **Суммарная оценка по дисциплине:** Сумма баллов текущей и промежуточной аттестации баллов. | | | | **51 – 100** |

## 5. Материально-техническое, программное и учебно-методическое обеспечение дисциплины.

### 5.1. Учебная литература

**Основная учебная литература**

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290.

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/538066

**Дополнительная литература**

1. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 252 с. — (Высшее

образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557730

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029.

3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132.

### 5.2. Материально-техническое и программное обеспечение дисциплины.

В обучении используются информационные технологии на базе компьютерных классов учебного корпуса №4 (пр. Металлургов 19):

- практические занятия по дисциплине проводятся с использованием программного обеспечения, приведенного в таблице 5.

Таблица 5 – Информационные технологии и программное обеспечение аудиторных занятий и самостоятельной работы

| Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы | Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения | Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом |
|---|---|---|
| 410 Учебная аудитория (мультимедийная) для проведения:<br>- занятий лекционного типа;<br>Специализированная (учебная) мебель: доска меловая, кафедра, моноблоки аудиторные.<br>Оборудование: стационарное - компьютер, экран, проектор.<br>Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС. | Специализированная (учебная) мебель: доска меловая, кафедра, моноблоки аудиторные.<br>Оборудование: стационарное - компьютер, экран, проектор.<br>Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС. | 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19 |
| 501 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения:<br>- занятий семинарского (практического) типа;<br>- групповых и индивидуальных | Специализированная (учебная) мебель: доска меловая, кафедра, столы компьютерные, стулья. Оборудование для презентации учебного материала: стационарное - компьютер преподавателя, экран, проектор. | 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19 |

| Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы | Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения | Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом |
|---|---|---|
| консультаций;<br>- самостоятельной работы;<br>- текущего контроля и промежуточной аттестации. | Оборудование: стационарное - компьютеры для обучающихся (17 шт.).<br>Используемое программное обеспечение: MS Windows (Microsoft Imagine Premium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), BloodshedDev C++ 4.9.9.2 (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Java (бесплатная версия), UML-диаграммы (бесплатная версия), Консультант Плюс (отечественное ПО, договор об инфо поддержке 1.04.2007), Oracle VM VirtualBox (бесплатная версия), Paint.NET (свободно распространяемое ПО).<br>Интернет с обеспечением доступа в ЭИОС. | |

**5.3. Современные профессиональные базы данных и информационные справочные системы.**

1. CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке -http://citforum.ru
2. Научная электронная библиотека eLIBRARY.RU – крупнейший российский информационный портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты - www.elibrary.ru.
3. Единое окно доступа к образовательным ресурсам - http://window.edu.ru/
4. База данных правовых актов «КонсультантПлюс»: комп. справ. правовая система / компания «КонсультантПлюс» . – URL: http://base.consultant.ru .– Режим доступа: свободный.

**6. Иные сведения и (или) материалы.**

**6.1. Примерные темы письменных учебных работ**

Письменные работы не предусмотрены.

## 6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 9 - Примерные теоретические вопросы и практические задания к экзамену

| Разделы и темы | Примерные теоретические вопросы | Примерные практические задания и (или) задачи |
|---|---|---|
| 1. Введение в предмет. Угрозы информационной безопасности. | 1. Что называется информационной безопасностью?<br>2. Какие данные называются критическими?<br>3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?<br>4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?<br>5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности? | *Задание 1.* Для одноалфавитного метода с задаваемым смешением выполнить шифрование с произвольным смещением. |
| 2. Основные понятия теории информационной безопасности. | 6. Перечислите меры защиты информационной безопасности?<br>7. Какие меры предпринимают по защите целостности информации?<br>8. Какие меры предпринимают по защите системных программ?<br>9. Дублирование информации и его классы.<br>10. Перечислите позиции административного уровня.<br>11. Назовите цель ОНРВ и его основные положения? | *Задание 2.* Для одноалфавитного метода с задаваемым смешением выполнить дешифрование зашифрованный шифром Цезаря текст. |
| 3. Программно-технические методы защиты. | 12. Что такое межсетевой экран и какая у него роль в защите.<br>13. Законодательная основа информационной безопасности, статьи и пр.<br>14. Что такое политика безопасности на административном уровне?<br>15. Основные принципы защиты информации на административном уровне?<br>Средства Разграничения доступа.<br>Что такое CGI процедуры, их назначения?<br>Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?<br>Как осуществляется защита WEB-серверов? | *Задание 3.* Проверить на простоту два произвольных целых числа разрядностью 5. |
| 4. Криптографические | 20. Криптография и | *Задание 4.* Задан интервал вида $[x, x + L]$. |

| Разделы и темы | Примерные теоретические вопросы | Примерные практические задания и (или) задачи |
|---|---|---|
| методы защиты. | криптоанализ. Назначение криптографии.<br>21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.<br>22. Симметричная и асимметричная методология шифрования.<br>23. Криптографические средства защиты.<br>24. Квантовая криптография и ККС. | Вычислить количество *П(x, L)* простых чисел в интервале и сравнить с величиной *L/1n(x)*. При каких условиях *П(x, L)/L* близко к *1/1n(x)* при заданных *x* = 2000, *L* = 500, количество простых чисел для деления 5-15, количество оснований 1-2? |
| 5. Организационно-правовые методы информационной безопасности. | 25. Чем определяется концепция обеспечения безопасности АСОИ.<br>26. В чем состоит избирательная политика безопасности способом управления доступом.<br>27. Организационные меры безопасности АСОИ.<br>28. Матрица доступа в АСОИ.<br>29 Полномочное управление доступом.<br>30. Избирательное управление доступом. | *Задание 5.* Найти в интервале (1000, 1000 + 300) все простые числа. Пусть L(i) - разность между двумя соседними простыми числами. Построить гистограмму для *L(i).* Вычислить выборочное среднее $L_{сред}$. Сравнить с величиной *1n(x)*, где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3. |
| 6. Роль стандартов в обеспечении информационной безопасности. | 31. Что такое универсальная операционная система?<br>32. Что такое компьютерный вирус.<br>33. Полиморфные вирусы.<br>34. Суррогатные платежные средства.<br>35. Файловые вирусы и алгоритм их работы.<br>36. Особенность макровирусов. | *Задание 6.* Для заданного набора чисел {*k*} оценить относительную погрешность формулы для *k*-го простого числа:<br>*p(k) = k/ln(k), k= {10, 15, 20, 30, 35}.* |
| 7. Технологии построения защищенных систем. | 37. Полномочное управление доступом.<br>38. Избирательное управление доступом.<br>39. Отказоустойчивые компьютерные системы.<br>40. Что вы понимаете под технологией RAID.<br>41.Методы дублирования информации. | *Задание 7.* В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые к простых. Расчет производится для всех *k* <= 10. |

Составитель (и): Штейнбрехер О.А., канд техн. наук, доцент кафедры информатики и вычислительной техники им. В.К. Буторина

(*фамилия, инициалы и должность преподавателя (ей)*)