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.04.06 Кибербезопасность

Направление подготовки
**01.04.02 Прикладная математика и информатика**

Направленность (профиль) подготовки
**МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ**

Программа магистратуры

Квалификация выпускника
*магистр*

Форма обучения
*Очная*

Год набора 2023

Новокузнецк 2024

## Оглавление

**1 Цель дисциплины.**

В результате освоения дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы магистратуры (далее - ОПОП): *ОПК-4*.

**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-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности | ОПК-4.3 Учитывает требования информационной безопасности при решении задач профессиональной деятельности | **Знать:**<br>– основные стандарты информационной безопасности.<br>**Уметь:**<br>– восстанавливать логи операционной системы и журнал просмотра веб-страниц с помощью специализированного ПО;<br>– проектировать архитектуру приложений в соответствии с требованиями информационной безопасности.<br>**Владеть:**<br>– навыками составления скриптов на языке YARA для определения вредоносного ПО. |

**Место дисциплины**

Дисциплина является факультативной дисциплиной и включена в модуль «Современные информационные технологии в профессиональной деятельности» ОПОП ВО. Дисциплина осваивается на 1 курсе во 2 семестре.

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

Таблица 2 – 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 | 72 |
| 2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего) | 32 |
| Аудиторная работа (всего): | 32 |
| в том числе: | |
| лекции | 16 |
| лабораторные занятия | 16 |
| 3 Самостоятельная работа обучающихся (всего) | 40 |
| 4 Промежуточная аттестация обучающегося<br>зачет (4 семестр) | |

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

**3.1 Учебно-тематический план**

Таблица 3 - Учебно-тематический план очной формы обучения

| № недели | Разделы и темы дисциплины по занятиям | Общая трудоёмкость | Трудоемкость занятий (час.) | Формы текущ. контроля и промежуточной аттестации |
|---|---|---|---|---|
| | | | ОФО | |

| | | (всего час.) | Аудиторн. занятия | | СРС | |
|---|---|---|---|---|---|---|
| | | | лекц. | лаб. | | |
| **Семестр 2** | | | | | | |
| 1. | 1. Кибербезопасность в «Интернет-вещей» и системах «Умного города» | 10 | 4 | | 6 | Презентация |
| 2. | 1.1 Кибербезопасность в «Интернет-вещей» для граждан | 5 | 2 | | 3 | |
| 3. | 1.2«Умный город»: состав систем | 5 | 2 | | 3 | |
| 4. | 2. Разработка архитектуры веб-сервиса | 14 | 2 | 2 | 10 | Индивидуальное задание |
| 5. | 3. Компьютерная криминалистика | 20 | 4 | 6 | 10 | Отчет о практической работе |
| 6. | 3.1 Сферы применения. Методология компьютерной криминалистики. | 9 | 2 | 2 | 5 | |
| 7. | 3.2 Роль специалистов ИКТ в компьютерной криминалистике. | 11 | 2 | 4 | 5 | |
| 8. | 4. Комплаенс в информационной безопасности | 18 | 2 | 2 | 6 | Презентация |
| 9. | 5. Целевые атаки в корпоративной среде | 26 | 4 | 6 | 8 | Отчет о практической работе |
| 10. | 5.1 Сбор данных об операциях целевого шпионажа, управление собранным знанием внутри компании и применение его для противодействия злоумышленникам. | 8 | 2 | 2 | 4 | |
| 11. | 5.2 Составление детектирующих правил на языке Yara, для проверки гипотез на парке всех серверов и эндпоинтов в компании. | 10 | 2 | 4 | 4 | |
| 6. | Промежуточная аттестация - зачет | | | | | |
| **ИТОГО по семестру 2** | | **72** | **16** | **16** | **40** | |

## 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 за освоение дисциплины (мин.-макс.) |
|---|---|---|---|---|
| Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий) | **80** | Практические работы (отчет о выполнении работы) (2 работы). | 7,5 баллов – выполнение задания на 51-85%<br>15 баллов – выполнение задания на 85,1-100%. | 15 – 30 |
| | | Индивидуальное задание | 6 баллов – выполнение задания на 51-85%<br>10 баллов – выполнение задания на 85,1-100%. | 6 - 10 |
| | | Презентация (2 работы) | 10 баллов – выполнение задания на 51-85%<br>20 баллов – выполнение задания на 85,1-100%. | 20 – 40 |
| **Итого по текущей работе в семестре** | | | | **41 – 80** |
| Промежуточная аттестация (зачет) | 20 | Теоретический вопрос | 2 балла (выполнено 70% заданий и более)<br>4 балла (выполнено 100% заданий ) | 2 - 4 |
| | | Практическое задание 1. | 4 балла - 8 баллов | 4 - 8 |
| | | Практическое задание 2. | 4 балла - 8 баллов | 4 - 8 |
| **Итого по промежуточной аттестации (зачету)** по приведенной шкале (20 б.) | | | | 10 – 20 б. |
| **Суммарная оценка по дисциплине 51 – 100 б.** | | | | |

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

### 5.1 Учебная литература

**Основная учебная литература**

Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512268.

Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927.

**Дополнительная учебная литература**

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084.

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

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

| | |
|---|---|
| **610** Учебная аудитория (мультимедийная)для проведения:<br>- занятий лекционного типа;<br>- текущего контроля и промежуточной аттестации.<br>**Специализированная (учебная) мебель:** доска меловая, кафедра, столы, стулья.<br>**Оборудование для презентации учебного материала**: стационарное - компьютер, экран, проектор.<br>**Используемое программное обеспечение:** LibreOffice (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО).<br>**Интернет с обеспечением доступа в ЭИОС**. | Учебный корпус №4.<br><br>654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19 |
| **501 Лаборатория программирования баз данных**.<br>Учебная аудитория (мультимедийная) для проведения:<br>- занятий лекционного типа;<br>- занятий семинарского (практического) типа;<br>- курсового проектирования (выполнения курсовых работ);<br>- групповых и индивидуальных консультаций;<br>- текущего контроля и промежуточной аттестации.<br>**Специализированная (учебная) мебель**: доска меловая, кафедра, столы компьютерные, стулья.<br>**Оборудование для презентации учебного материала**: *стационарное* - компьютер преподавателя, экран, проектор.<br>**Лабораторное оборудование**: *стационарное* - компьютеры для обучающихся (17 шт.).<br>**Используемое программное обеспечение**: LibreOffice (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Android Studio.<br>**Интернет с обеспечением доступа в ЭИОС.** | Учебный корпус №4.<br><br>654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19 |

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

**Перечень СПБД и ИСС по дисциплине**

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 База данных Science Direct (более 1500 журналов издательства Elsevier, среди них издания по математике и информатике), режим доступа :https://www.sciencedirect.com.

## 6 Иные сведения и (или) материалы.

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

Форма промежуточной аттестации экзамен.

Таблица 5 – Типовые (примерные) контрольные вопросы и задания

| Разделы и темы | Примерные теоретические вопросы | Примерные практические задания и (или) задачи |
|---|---|---|
| Семестр 2 зачет | | |
| 1. Кибербезопасность в «Интернет-вещей» и системах «Умного города» | 1. Кибербезопасность в «Интернет-вещей» для граждан: классификация продуктов «Интернет-вещей» для граждан, угрозы, уязвимости, риски на примере популярных продуктов.<br>2. «Интернет-вещей» в сфере здравоохранения – риски и проблемы.<br>3. «Умный дом» - риски и проблемы.<br>4. «Интернет-вещей» и его применение в Smart Grid, проблемы кибербезопасности.<br>5. «Умный город»: состав систем (категории систем, классификация).<br>6. Зрелость Smart City: понятие, критерии оценки, угрозы, риски и проблемы, модель угроз (структура, особенности).<br>7. Стандарты по направлению «Умный город» (Smart City). | 1. В зависимости от места хранения данных в системе IoT эксперты в сфере IoT криминалистики выделяют три опасных участка в ландшафте киберугроз. Опишите эти участки. Предложите способы защиты.<br>2. Какие активы в системе IoT требуют защиты? Определите возможные угрозы системе IoT. |
| 2. Разработка архитектуры веб-сервиса | 8. Модель нарушителя.<br>9. Наиболее распространённые проблемы безопасности веб-приложений.<br>10. Хранение паролей.<br>11. Защита от XSS и CSRF.<br>12. Безопасные алгоритмы хеширования: Argon2.<br>13. Аутентификация пользователей. Cookie-based auth, Token-based auth.<br>14. Аутентификация пользователей.<br>15. Аутентификация без паролей: Webauthn, по номеру телефона.<br>16. Безопасное взаимодействие между различными сервисами.<br>17. Обработка пользовательских данных. | 3. Составьте схему Cookie-based auth.<br>4. Составьте схему Token-based auth.<br>5. Опишите риски использования аутентификации пользователей по номеру телефона.<br>6. Проверьте уязвимость веб-сервиса к SQL-инъекциям. |
| 3. Компьютерная криминалистика | 18. Сферы применения компьютерной криминалистики. | 7. Установите список посещаемых сайтов по |

| | | |
|---|---|---|
| | 19. Методология компьютерной криминалистики.<br>20. Специальные методы исследования.<br>21. Формы методов компьютерной криминалистики.<br>22. Роль специалистов ИКТ в компьютерной криминалистике.<br>23. Роль экспертно-криминалистических подразделений. | сохраненным данным браузера с помощью программы «EnCase».<br>8. Установите список посещаемых сайтов по сохраненным данным браузера с помощью программы «FTK».<br>9. Установите список посещаемых сайтов по сохраненным данным браузера с помощью программы «Pasco».<br>10. Соберите логи Windows с помощью программы «Event Viewer». |
| 4. Комплаенс в информационной безопасности | 24. «Бумажная» и «практическая» безопасность.<br>25. Формирование сведений об угрозах безопасности информации<br>26. Формирование возможных последствий. Требования по информационной безопасности.<br>27. Комплаенс. Построение процессов и риски.<br>28. Комплаенс. Менеджмент. | 11. Выявите требования по информационной безопасности IT-компании.<br>12. Выявите требования по информационной безопасности университета. |
| 5. Целевые атаки в корпоративной среде | 29. Массовые атаки.<br>30. Целевые атаки.<br>31. Поиск целевых угроз: профилирование. | 13. Напишите на языке YARA скрипт, который ищет в файлах содержимое: $str1=" gethostpoop fuxore ".<br>14. Напишите на языке YARA скрипт, который ищет в файлах содержимое: $str1=" nc -l -p port [options] ". |
| **Компетенции** | | |
| ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности | Задание 1<br>В предметной области «Учет личных дел студентов университета» сформулируйте требования по информационной безопасности.<br>- Разработайте проект личного кабинета студента: сервис хранения паролей, авторизация, просмотр расписания, просмотр новостей университета.<br>Задание 2<br>Дан сайт некоторой организации.<br>- Сформулируйте требования по информационной безопасности.<br>- Проверьте сайт организации на наличие уязвимости к SQL-инъекциям. | |

Составитель (и): старший преподаватель кафедры МФММ Гаврилова Ю.С.

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