Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

# РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

*«ФДТ.4 Методология кибериммунитета»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

*02.03.02 Фундаментальная информатика и информационные технологии*
(код и наименование направления подготовки)

*Разработка корпоративных систем и цифровых решений*
(наименование направленности (профиля) образовательной программы)

Квалификация

*Бакалавр*

Форма обучения

*Очная*

Год набора 2026

Рабочая программа дисциплины «*ФДТ.4 Методология кибериммунитета*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
*наименование кафедры*

протокол № _____ от "___" _____ 20__ г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
*наименование кафедры* *подпись* И.В. Влацкая *расшифровка подписи*

*Исполнители:*
Доцент *должность* *подпись* И.В. Влацкая *расшифровка подписи*

*должность* *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.02 Фундаментальная информатика и информационные технологии
*код наименование* *личная подпись* И.П. Болодурина *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
главный библиотекарь *личная подпись* Г.С. Гайтис *расшифровка подписи*

Уполномоченный по качеству института
*личная подпись* С.Н. Морозова *расшифровка подписи*

№ регистрации _____

© Влацкая И.В., 2026
© ОГУ, 2026

## 1 Цели и задачи освоения дисциплины

**Цель** освоения дисциплины: получение знаний в области кибериммунной разработки программного обеспечения, которая позволяет защищать пользовательские системы от угроз уже на этапе проектирования.

**Задачи:**
- освоить основные принципы кибериммунной разработки программных продуктов;
- уметь разрабатывать политики безопасности систем;
- уметь создавать позитивные и негативные сценарии тестирования программного средства.

## 2 Место дисциплины в структуре образовательной программы

Дисциплина является факультативной(ым)

Пререквизиты дисциплины: *Б1.Д.Б.11 Основы программирования*

Постреквизиты дисциплины: *Отсутствуют*

## 3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности | ОПК-5-В-4 Соблюдает требования информационной безопасности | **Знать:**<br>- содержание концепции безопасности продукта и критерии оценки её качества;<br>- особенности политики безопасности архитектуры программного продукта; основные виды политик управления доступом и информационными потоками в компьютерных системах.<br><br>**Уметь:**<br>- анализировать и оценивать угрозы информационной безопасности объекта;<br>- оценить качество концепции безопасности продукта по заданным критериям. |

| Код и наименование формируемых компетенций | Код и наименование индикатора достижения компетенции | Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций |
|---|---|---|
| | | **Владеть:**<br>- навыками построения формальных моделей управления доступом, моделей изолированной программной среды и безопасности информационных потоков;<br>- навыками создания тестов безопасности на основе аналогичных примеров. |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

| Вид работы | Трудоемкость, академических часов | |
|---|---|---|
| | 7 семестр | всего |
| **Общая трудоёмкость** | **108** | **108** |
| **Контактная работа:** | **34,25** | **34,25** |
| Лекции (Л) | 18 | 18 |
| Лабораторные работы (ЛР) | 16 | 16 |
| Промежуточная аттестация (зачет, экзамен) | 0,25 | 0,25 |
| **Самостоятельная работа:**<br>*- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);*<br>*- изучение разделов курса «Методология кибериммунитета» в системе электронного обучения;*<br>*- подготовка к итоговому тестированию в системе электронного обучения;*<br>*- подготовка к лабораторным занятиям;*<br>*- подготовка к рубежному контролю.* | **73,75** | **73,75** |
| **Вид итогового контроля (зачет, экзамен, дифференцированный зачет)** | **зачет** | |

Разделы дисциплины, изучаемые в 7 семестре

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 1 | Введение. Цели и актуальные задачи курса «Методология кибериммунитета». | 20 | 2 | | 2 | 16 |

| № раздела | Наименование разделов | Количество часов | | | | |
|---|---|---|---|---|---|---|
| | | всего | аудиторная работа | | | внеауд. работа |
| | | | Л | ПЗ | ЛР | |
| 2 | Информационная безопасность. Угрозы информационной безопасности. Защита информации. Банк данных угроз ФСТЭК. | 22 | 4 | | 4 | 14 |
| 3 | Кибериммунитет. Концепция безопасного продукта. | 20 | 4 | | 2 | 14 |
| 4 | Кибериммунные системы. Проблемы разработки кибериммунных систем. | 18 | 2 | | 2 | 14 |
| 5 | Проектирование кибериммунной системы. | 28 | 6 | | 6 | 16 |
| | Итого: | 108 | 18 | | 16 | 74 |
| | Всего: | 108 | 18 | | 16 | 74 |

**4.2 Содержание разделов дисциплины**

**Раздел 1. Введение. Цели и актуальные задачи курса «Методология кибериммунитета».**

Цель и задачи курса. Место факультативной дисциплины в образовательном процессе. Кибериммунный подход. Основные термины и определения. технологии кибериммунитета**.**

**Раздел 2. Информационная безопасность и кибербезопасность.**

Основные термины и определения в области компьютерной безопасности. Угрозы информационной безопасности. Банк данных угроз. Методика ФСТЭК.

**Раздел 3. Кибериммунитет. Концепция безопасного продукта.**

Понятие безопасного продукта. Шаблон описания безопасного продукта. Цели и предположения безопасности. Анализ угроз. Декомпозиция системы. Доверенные, недоверенные компоненты. Архитектурные диаграммы. Политики безопасности. Технология изолированного проектирования компонент кибериммунной системы. Управление политикой безопасности.

**Раздел 4. Кибериммунные системы. Проблемы разработки кибериммунных систем.**

Требования к архитектуре. Требования к процессу. Выбор окружения. Средства разработки. Анализ и подбор сторонних утилит. Политика безопасности. Негативные сценарии. Анализ полученной модели.

**Раздел 5. Проектирование кибериммунной системы.**

Верификация и тестирование. Моделирование угроз. Распределение обязанностей на всех этапах проектирования кибериммунной системы. Типичные ошибки проектирования.

Концепция безопасности программного продукта. Цели и предположения безопасности. Описание компонент системы. Схема взаимодействия компонент системы. Построение диаграммы последовательности. Описание негативных сценариев. Верификация компонент системы для обеспечения политики безопасности.

Цели и предположения безопасности. Негативные сценарии. Архитектура и диаграмма потоков данных (DFD). Политики безопасности. Тесты (функциональные и безопасности).

### 4.3 Лабораторные работы

| № ЛР | № раздела | Наименование лабораторных работ | Кол-во часов |
|---|---|---|---|
| 1 | 1 | Разработка диаграмм последовательности для различных систем. | 2 |
| 2 | 2 | Работа с БДУ ФСТЭК. | 4 |
| 3 | 1, 2 | Создание описания безопасного продукта для пользовательской системы (на основе шаблона). | 2 |
| 4 | 2, 3 | Разработка архитектуры системы. Использование технологии MILS для обеспечения изолированности компонент системы. | 4 |
| 5 | 3, 4, 5 | Разработка архитектуры системы. Описание негативных сценариев. Декомпозиция архитектуры системы. Минимизация доверенной базы компонент. | 4 |
| | | Итого: | 16 |

## 5 Учебно-методическое обеспечение дисциплины

### 5.1 Основная литература

1. Мельников, В. П. Информационная безопасность и защита информации [Текст]: учебное пособие для студентов высших учебных заведений, обучающихся по специальности "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 6-е изд., стер. - Москва: Академия, 2012. - 332 с.: ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-9222-5.

2. Малюк, А. А. Введение в защиту информации в автоматизированных системах [Текст]: учеб. пособие для студентов, обучающихся по спец., не входящим в группу спец. в обл. информ. безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин.- 2-е изд. - М. : Горячая линия-Телеком, 2004. - 147 с.: ил. - Библиогр.: с. 143. - ISBN 5-93517-062-0.

### 5.2 Дополнительная литература

1. Байбурин В.Б. Введение в защиту информации [Текст]: учеб. пособие для вузов / В.Б. Байбурин [и др.]. - М.: ФОРУМ: ИНФРА-М, 2004. - 128 с. - Библиогр.: с. 124-125. - ISBN 5-89199-0130-4. - ISBN 5-16-001942-1.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин. - Москва: Форум: ИНФРА-М, 2014. - 416 с.: ил. - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3.

### 5.3 Периодические издания

Журналы:

– Информационная безопасность, издательство компании «Гротек», г. Москва. Режим доступа: https://lib.itsec.ru/imag/

– Проблемы информационной безопасности. Компьютерные системы, издательство СпбПУ, г. Санкт-Петербург. Режим доступа: https://jisp.spbstu.ru/archive/

### 5.4 Интернет-ресурсы

1. Flask security architecture https://www.cs.cmu.edu/~dga/papers/flask-usenixsec99.pdf
2. MILS Architectural Approach Supporting Trustworthiness of the IIoT Solutions https://www.iiconsortium.org/pdf/MILS-Architectural-Approach-Supporting-Trustworthiness-of-IIoT-Solutions-Whitepaper.pdf
3. Кибериммунитет Кибериммунитет · sergey-sobolev/cyberimmune-systems Wiki (github.com)
4. SecurityLab.ru. Режим доступа: http://www.securitylab.ru
5. Открытые системы. Режим доступа: http://www.osp.ru
6. CIT FORUM. Режим доступа: http://www.citforum.ru

**Стандарты:**

– ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

– ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»

– ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (утв. и введен в действие Приказом Росстандарта от 15.11.2012 № 814-ст).

– ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Часть 2. Функциональные компоненты безопасности.

– ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

– ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

– ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

– ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования».

– ГОСТ 29099-91. «Сети вычислительные локальные. Термины и определения».

– ISO/IEC 27001:2005. «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». 2012 г.

– ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью». 2013 г.

– ISO/IEC 27006:2007 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью».

– ГОСТ Р 72118:2025 «Системы с конструктивной информационной безопасностью. Методология разработки».

### 5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

– Операционная система Astra Linux. «Astra Linux Special Edition» РУСБ.10015-01, лицензионный договор №А-2021-1374-ВУЗ от 28.05.2021;

– Пакет офисных приложений «МойОфис Образование».

Базы данных, информационно-справочные и поисковые системы:

- Консультант Плюс, Режим доступа: https://www.consultant.ru/cons/cgi/online.cgi
- Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/

## 6 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами. Рабочие станции студентов и преподавателя объединены в локальную компьютерную сеть с возможностью выхода в Интернет.

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием.

Лабораторные занятия проходят в компьютерных классах, в которых установлено оборудование:

- системные блоки на базе процессора Intel Core i5;
- системные блоки на базе процессора Intel Pentium Core 2 Duo;
- мониторы моделей Samsung, ViewSonic.

***К рабочей программе прилагаются:***

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.