

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

## **РАБОЧАЯ ПРОГРАММА**

**ДИСЦИПЛИНЫ**

*«ФДТ.4 Методология кибериммунитета»*

Уровень высшего образования

**БАКАЛАВРИАТ**

Направление подготовки

*15.03.04 Автоматизация технологических процессов и производств*

(код и наименование направления подготовки)

*Системы автоматизации технологических процессов и производств*

(наименование направленности (профиля) образовательной программы)

Квалификация

*Бакалавр*

Форма обучения

*Очная*

Год набора 2023

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

Кафедра компьютерной безопасности и математического обеспечения информационных систем  
наименование кафедры

протокол № 8 от "25" марта 2024г.

Заведующий кафедрой

Кафедра компьютерной безопасности и математического обеспечения информационных систем

наименование кафедры

подпись

расшифровка подписи

Исполнители:

Доцент

должность

подпись

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

15.03.04 Автоматизация технологических процессов и производств

код наименование

личная подпись

расшифровка подписи

Д.А. Проскурин

/ Заведующий отделом формирования фонда и научной обработки документов

личная подпись

Н.Н. Бигалиева

Е.А. Биктимирова

Уполномоченный по качеству факультета

личная подпись

И.В. Крючкова

№ регистрации \_\_\_\_\_

## 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.12 Информатика*

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-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4-В-1 Изучает современные информационные технологии и программные средства для решения задач профессиональной деятельности ОПК-4-В-2 Анализирует принципы работы современных информационных технологий для решения задач профессиональной деятельности ОПК-4-В-3 Решает задачи профессиональной деятельности с использованием современных информационных технологий	<b>Знать:</b> - содержание концепции безопасности продукта и критерии оценки её качества; - особенности политики безопасности архитектуры программного продукта; основные виды политик управления доступом и информационными потоками в компьютерных системах.  <b>Уметь:</b> - анализировать и оценивать угрозы информационной безопасности объекта; - 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
		<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- навыками построения формальных моделей управления доступом, моделей изолированной программной среды и безопасности информационных потоков;</li> <li>- навыками создания тестов безопасности на основе аналогичных примеров.</li> </ul>

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

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».	16	2		2	12
2	Информационная безопасность. Угрозы	18	4		4	10

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
	информационной безопасности. Защита информации. Банк данных угроз ФСТЭК.					
3	Кибериммунитет. Концепция безопасного продукта.	16	4		2	10
4	Кибериммунные системы. Проблемы разработки кибериммунных систем.	14	2		2	10
5	Проектирование кибериммунной системы.	14	2		2	10
6	Пример проектирования кибериммунной системы, выполняющей обновление приложений на базе микросервисной архитектуры.	14	2		2	10
7	Разбор решений учебных примеров лаборатории Касперского	16	2		2	12
	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.

### **Раздел 6. Пример проектирования кибериммунной системы, выполняющей обновление приложений на базе микросервисной архитектуры.**

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.

### **Раздел 7 Разбор решений учебных примеров лаборатории Касперского.**

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	Создание описания безопасного продукта для пользовательской системы (на основе шаблона).	2
4	2	Разработка архитектуры системы. Использование технологии MILS для обеспечения изолированности компонент системы.	2
5	2	Управление политикой безопасности с помощью системы FLASK.	2
6	3, 4	Разработка архитектуры системы. Описание негативных сценариев. Декомпозиция архитектуры системы. Минимизация доверенной базы компонент.	2
7	5	Разбор учебных примеров.	2
		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. Байбурун В.Б. Введение в защиту информации [Текст]: учеб. пособие для вузов / В.Б. Байбурун [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;

- Вестник информационной безопасности, издательство компании «Гротек», г. Москва;
- Проблемы информационной безопасности. Компьютерные системы, издательство СПбПУ, г. Санкт-Петербург.

#### 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 \(github.com\)](https://github.com/sergey-sobolev/cyberimmune-systems)
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».

#### 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;
- LibreOffice – свободно распространяемый офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.

Базы данных, информационно-справочные и поисковые системы:

- Консультант Плюс, Режим доступа: <https://www.consultant.ru/cons/cgi/online.cgi>
- Открытые поисковые системы: Yandex, Mail и др.

## **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.