Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «КИБЕРИММУННЫЙ ПОДХОД К РАЗРАБОТКЕ ПО»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Интеллектуальные цифровые системы и сервисы в управлении

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Арапова Ю. В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Менеджер по информационным технологиям", утвержден приказом Минтруда России от 30.08.2021 № 588н; "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Системный аналитик", утвержден приказом Минтруда России от 27.04.2023 № 367н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра прикладной информатики	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Ермолина Л. В.	Рассмотрено	21.05.2026, № 9

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся теоретических знаний и практических навыков в области кибериммунного подхода к разработке программного обеспечения, обеспечивающих способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и учитывать основные требования информационной безопасности при решении профессиональных задач

Задачи изучения дисциплины:

- Освоение теоретических основ кибериммунного подхода к разработке ПО;
- Формирование навыков применения ИКТ для решения профессиональных задач с учётом требований информационной безопасности;
- Развитие компетенций в области информационно-библиографической культуры при разработке безопасного ПО.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

Знать:

ОПК-3.1/Зн1 Методы информационной культуры и ИКТ для решения профессиональных задач

Уметь:

ОПК-3.1/Ум1 Применять ИКТ для поиска, анализа и решения стандартных задач

Владеть:

ОПК-3.1/Нв1 Навыками использования ИКТ и библиографических источников

ОПК-3.2 Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности

Знать:

ОПК-3.2/Зн1 Основные требования информационной безопасности, виды угроз и уязвимостей ПО, методы защиты информации и обеспечения безопасности на этапах разработки и эксплуатации, нормативные документы в области ИБ

Уметь:

ОПК-3.2/Ум1 Учитывать требования информационной безопасности при решении профессиональных задач, идентифицировать риски и угрозы для разрабатываемого ПО, применять методы защиты информации и контроля доступа

Владеть:

ОПК-3.2/Нв1 Навыками обеспечения информационной безопасности при разработке ПО, методами анализа уязвимостей и оценки рисков, способами применения защитных механизмов в рамках кибериммунного подхода

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Кибериммунный подход к разработке ПО» относится к обязательной части образовательной программы и изучается в семестре(ах): 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ОПК-3 - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Современные цифровые платформы	Выполнение и защита выпускной квалификационной работы, Информационная безопасность, Надежность интеллектуальных систем, Производственная практика: преддипломная практика
ОПК-3.2 Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности		Выполнение и защита выпускной квалификационной работы, Информационная безопасность, Надежность интеллектуальных систем, Производственная практика: преддипломная практика

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Групповая контактная работа (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Четвертый семестр	108	3	54	36	18	2	0,3	17,7	Экзамен
Всего	108	3	54	36	18	2	0,3	17,7	34

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лабораторные занятия	Лекционные занятия	Самостоятельная работа

Раздел 1. Основы кибериммунной разработки программного обеспечения	**71,7**	**36**	**18**	**17,7**
Тема 1.1. Введение в кибериммунный подход. Основные понятия, принципы и стандарты	8	4	2	2
Тема 1.2. Угрозы и уязвимости программного обеспечения. Методы анализа рисков	16	8	4	4
Тема 1.3. Механизмы реализации кибериммунного подхода, защита по умолчанию, минимальные привилегии	16	8	4	4
Тема 1.4. Управление безопасностью на этапах жизненного цикла ПО	16	8	4	4
Тема 1.5. Применение кибериммунного подхода в современных ИТ-решениях	15,7	8	4	3,7

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Основы кибериммунной разработки программного обеспечения	Тестирование	Экзамен

6. Оценочные материалы текущего контроля

1. Основы кибериммунной разработки программного обеспечения Тестирование

№ п/п	Содержание вопроса / Правильный ответ (ключ ответа)	Компетенция
1	Выберите один вариант ответа Что из перечисленного является ключевым принципом кибериммунного подхода к разработке ПО? а) Использование только открытого программного обеспечения б) Изоляция компонентов системы друг от друга и от внешней среды в) Постоянное обновление антивирусных баз г) Размещение всех данных в облачном хранилище Ответ: б	ОПК-3
2	Выберите один вариант ответа Какая операционная система разработана по принципу Secure by Design и является основой для создания кибериммунных решений? а) Windows б) Linux в) KasperskyOS г) macOS Ответ: в	ОПК-3

3	Выберите один вариант ответа Что такое минимизация доверенной вычислительной базы (ДВБ) в контексте кибериммунного подхода? а) Уменьшение количества пользователей, имеющих доступ к системе б) Сокращение объёма кода и компонентов, которые должны быть безусловно надёжными в) Установка минимального количества антивирусных программ г) Ограничение времени работы системы Ответ: б	ОПК-3
4	Выберите один вариант ответа Какой из перечисленных стандартов используется при создании кибериммунных решений? а) ГОСТ Р ИСО/МЭК 12207 б) Common Criteria в) IEEE 802.11 г) RFC 791 Ответ: б	ОПК-3
5	Выберите один вариант ответа Для решения стандартной задачи поиска научной литературы по теме «Кибериммунная разработка ПО» наиболее эффективно использовать: а) Поисковую систему Яндекс б) Научную электронную библиотеку eLibrary.ru в) Социальную сеть «ВКонтакте» г) Википедию Ответ: б	ОПК-3
6	Установите соответствие Соотнесите принцип кибериммунного подхода с его описанием: Принцип — Описание 1. Изоляция компонентов — А. Система сохраняет работоспособность даже при наличии атак 2. Минимизация ДВБ — Б. Система делится на части (домены), изолированные друг от друга 3. Secure by Design — В. Безопасность закладывается на этапе проектирования, а не добавляется позже 4. Устойчивость к атакам — Г. Сокращение объёма кода, который должен быть безусловно надёжным Ответ: 1-Б, 2-Г, 3-В, 4-А.	ОПК-3
7	Установите соответствие Соотнесите вид угрозы информационной безопасности с примером её реализации: Угроза — Пример 1. Вредоносное ПО — А. Поддельное письмо от «банка» с просьбой ввести логин и пароль 2. Социальная инженерия — Б. Программа-шифровальщик, блокирующая доступ к файлам 3. DDoS-атака — В. Злоумышленник подбирает пароль к учётной записи 4. Брутфорс — Г. Перегрузка сервера большим количеством ложных запросов Ответ: 1-Б, 2-А, 3-Г, 4-В.	ОПК-3
8	Установите соответствие Соотнесите вид информационно-коммуникационной технологии с её назначением: Технология — Назначение 1. Система управления базами данных (СУБД) — А. Организация совместной работы над документами 2. Облачные платформы (Яндекс.Облако, Google Cloud) — Б. Хранение и структурированное извлечение данных 3. Библиографические базы данных (eLibrary, Scopus) — В. Поиск и анализ научных публикаций 4. Средства совместной работы (Google Docs) — Г. Хранение и обработка данных с удалённым доступом Ответ: 1-Б, 2-Г, 3-В, 4-А.	ОПК-3
9	Установите правильную последовательность Расположите этапы проектирования кибериммунной системы в правильном порядке: 1. Определение доменов безопасности и изоляция компонентов 2. Анализ угроз и рисков для разрабатываемой системы 3. Разработка политик взаимодействия между компонентами 4. Реализация и тестирование системы 5. Формулирование требований к безопасности на этапе проектирования Ответ: 5, 2, 1, 3, 4.	ОПК-3
10	Установите правильную последовательность Расположите шаги выполнения библиографического поиска в правильном порядке: 1. Оценка релевантности и качества найденных источников 2. Формулирование темы и ключевых слов для поиска 3. Оформление списка литературы в соответствии с требованиями 4. Поиск в специализированных базах данных (eLibrary, Google Scholar, Scopus) 5. Сохранение найденных источников с использованием библиографического менеджера Ответ: 2, 4, 1, 5, 3.	ОПК-3

11	Дайте верный ответ Опишите три основных принципа кибериммунного подхода к разработке ПО. Для каждого принципа приведите пример его реализации в архитектуре системы.		ОПК-3
	Ответ:	1. Изоляция компонентов 2. Минимизация доверенной вычислительной базы (ДВБ) 3. Secure by Design	
12	Дайте верный ответ Вам необходимо найти актуальные научные публикации по теме «Методы обеспечения кибериммунности встроенных систем». Опишите последовательность действий с указанием конкретных информационно-коммуникационных технологий и библиографических источников, которые вы будете использовать.		ОПК-3
	Ответ:	1. Сформулирую ключевые слова: «кибериммунность», «встроенные системы», «secure by design», «изоляция компонентов». 2. Выполню поиск в научных электронных библиотеках: eLibrary.ru (российские публикации), Google Scholar и Scopus (международные). 3. Отфильтрую результаты по релевантности, цитируемости и дате публикации (за последние 5 лет). 4. Сохраню найденные источники с помощью библиографического менеджера Mendeley. 5. Оформлю список литературы в соответствии с ГОСТ 7.1-2003 (или актуальной версией).	
13	Дайте верный ответ Разработайте план мероприятий по обеспечению информационной безопасности на этапе разработки ПО с использованием кибериммунного подхода. План должен включать не менее 5 этапов с обоснованием каждого.		ОПК-3
	Ответ:	1. Анализ угроз и моделирование атак 2. Проектирование архитектуры с изоляцией компонентов 3. Разработка политик взаимодействия 4. Реализация с использованием безопасных языков и практик программирования 5. Тестирование безопасности (пен-тестирование, анализ уязвимостей) —	
14	Дайте верный ответ Сравните традиционный подход к обеспечению информационной безопасности (защита «периметра») и кибериммунный подход. В чём ключевые различия? Приведите не менее трёх отличий.		ОПК-3
	Ответ:	1. Время обеспечения безопасности 2. Реакция на атаки 3. Архитектура	
15	Дайте верный ответ Опишите, как применение кибериммунного подхода может снизить риски, связанные с «неизвестными уязвимостями» (zero-day).		ОПК-3
	Ответ:	Кибериммунный подход снижает риски zero-day уязвимостей за счёт изоляции компонентов: даже если злоумышленник найдёт уязвимость в одном компоненте, он не сможет получить доступ к другим частям системы. Кроме того, минимизация доверенной вычислительной базы сокращает количество кода, в котором могут быть обнаружены уязвимости. Контроль взаимодействий между компонентами не позволяет атакующему развить атаку и получить контроль над всей системой	

7. Оценочные материалы промежуточной аттестации

Экзамен четвертый семестр

№ п/п	Содержание вопроса	Правильный ответ (ключ ответа)	Компетенция
1	Дайте развернутый ответ Дайте определение кибериммунного подхода к разработке ПО. Перечислите его основные принципы.		ОПК-3
	Ответ:	Кибериммунный подход — методология разработки ПО, позволяющая создавать системы, устойчивые к кибератакам даже при наличии неизвестных уязвимостей. Основные принципы: изоляция компонентов, минимизация доверенной вычислительной базы, Secure by Design, контроль взаимодействий между компонентами	
2	Дайте развернутый ответ Что такое «изоляция компонентов» в кибериммунном подходе и почему она важна для информационной безопасности?		ОПК-3
	Ответ:	Изоляция компонентов — это разделение системы на изолированные части (домены), каждая из которых имеет строго определённые права доступа. Это важно, потому что даже при компрометации одного компонента злоумышленник не может получить доступ к другим частям системы, что ограничивает распространение атаки	
3	Дайте развернутый ответ Какие информационно-коммуникационные технологии вы будете использовать для поиска и анализа научной литературы по теме «Кибериммунная разработка ПО»?		ОПК-3
	Ответ:	Буду использовать научные электронные библиотеки (eLibrary.ru, Google Scholar, Scopus), системы управления библиографией (Mendeley, Zotero), а также поисковые системы с расширенными возможностями фильтрации. Методика: формулирование ключевых слов → поиск → фильтрация по релевантности и цитируемости → сохранение источников → оформление списка литературы по ГОСТ.	
4	Дайте развернутый ответ Какие стандарты и нормативные документы регулируют создание кибериммунных систем?		ОПК-3

	Ответ:	Common Criteria, ASPICE, ISO 26262. Эти стандарты определяют требования к безопасности на всех этапах жизненного цикла разработки. KasperskyOS соответствует указанным стандартам	
5	Дайте развернутый ответ Опишите навыки работы с библиографическими источниками, необходимые для решения стандартных задач профессиональной деятельности		ОПК-3
	Ответ:	Навыки включают: формулирование поисковых запросов, работу с научными базами данных (eLibrary, Scopus), критический анализ источников, использование библиографических менеджеров (Mendeley, Zotero), оформление списка литературы в соответствии с ГОСТ 7.1-2003, оценку релевантности и достоверности источников.	
6	Дайте развернутый ответ Как учитывать требования информационной безопасности при разработке ПО с использованием кибериммунного подхода?		ОПК-3
	Ответ:	Требования ИБ учитываются на всех этапах: анализ угроз на этапе проектирования, изоляция компонентов, минимизация доверенной вычислительной базы, разработка политик взаимодействия, тестирование безопасности, использование Secure by Design	
7	Дайте развернутый ответ Какие методы анализа уязвимостей применяются в кибериммунном подходе?		ОПК-3
	Ответ:	Моделирование угроз, анализ векторов атак, статический и динамический анализ кода, пен-тестирование, анализ контрольных сумм и целостности данных, проверка политик взаимодействия между компонентами.	
8	Дайте развернутый ответ Что такое «микроядро» и какую роль оно играет в кибериммунной архитектуре?		ОПК-3
	Ответ:	Микроядро — минимальный набор функций, необходимых для работы системы, разработанный с акцентом на безопасность. В кибериммунной архитектуре микроядро обеспечивает изоляцию компонентов и контроль взаимодействий, являясь минимальной доверенной вычислительной базой.	
9	Дайте развернутый ответ Какие методы информационной культуры применяются при решении профессиональных задач в области разработки ПО?		ОПК-3
	Ответ:	Работа с научной литературой, поиск в специализированных базах данных, критический анализ информации, использование систем управления знаниями, оформление результатов исследований в соответствии с требованиями, применение ИКТ для автоматизации рутинных задач.	
10	Дайте развернутый ответ Опишите сценарий атаки на систему, не обладающую кибериммунностью, и объясните, как кибериммунный подход предотвращает развитие этой атаки.		ОПК-3
	Ответ:	В традиционной системе атакующий может через уязвимость в одном компоненте получить доступ к другим частям системы и развить атаку. В кибериммунной системе изоляция компонентов и контроль взаимодействий не позволяют атакующему распространиться на другие домены. Система продолжает выполнять критические функции даже в условиях агрессивной среды.	

7.1. Уровни овладения

Компетенция: ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Индикатор достижения компетенции: ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80

Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: ОПК-3.2 Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Кириченко, А.А. Операционные системы. Практикум: Учебное пособие / А.А. Кириченко, С.В. Назаров, Л.П. Гудыно. - Москва: КноРус, 2020. - 372 с. - 978-5-406-07707-8. - Текст: электронный // book_ru: [сайт]. - URL: https://book.ru/book/933567 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Гаврилов, М. В. Архитектура ЭВМ и системное программное обеспечение: учебник для вузов / М. В. Гаврилов, В. А. Климов. - 6-е изд. - Москва: Юрайт, 2026. - 84 с - 978-5-534-20334-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589930 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Чернышев, С. А. Принципы, паттерны и методологии разработки программного обеспечения: учебник для вузов / С. А. Чернышев. - Москва: Юрайт, 2026. - 176 с - 978-5-534-14383-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588769 (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://minfin.gov.ru/ - Министерство финансов Российской Федерации (Минфин России)
2. http://www.gks.ru/ - Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики

Ресурсы «Интернет»

1. http://www.gov.ru - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия"

2. https://cyberleninka.ru/ - Научная электронная библиотека «КиберЛенинка»

3. https://www.planetaexcel.ru/ - Планета Excel

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СП
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения