ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«25» мая 2026 г.
Протокол № 2

Рабочая программа дисциплины (модуля)
«Информационная безопасность»

Направление подготовки: *02.04.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Управление командами разработки*

Квалификация (степень) выпускника: *магистр*

Форма обучения: *очная*

Срок освоения программы: *2 года*

Год набора: *2026*

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Москва
2026

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению 02.04.01 Математика и компьютерные науки, профиль Управление командами разработки, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 810 от 23.08.2017 года.

Изучение дисциплины (модуля) «Информационная безопасность» позволяет сформировать способность разрабатывать программное обеспечение с встроенными механизмами защиты, внедрять инструменты обнаружения уязвимостей в производственный процесс и реализовывать меры безопасности на архитектурном уровне.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки магистратуры по направлению 02.04.01 Математика и компьютерные науки, профиль Управление командами разработки и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений как дисциплина по выбору.

Дисциплина (модуль) изучается на 2 курсе в 3 семестре. Доступна к прохождению после успешного освоения дисциплин (модулей) «Алгоритмы и структуры данных», «Инструменты разработчика».

Цель изучения дисциплины (модуля): формирование у студентов комплексных знаний и практических навыков обеспечения защиты программных систем, включая применение криптографических методов, анализ уязвимостей и внедрение безопасных решений на всех этапах жизненного цикла разработки.

Задачи изучения дисциплины (модуля):

- освоить основные принципы и методы обеспечения информационной безопасности программных систем;
- изучить современные криптографические алгоритмы и сценарии их применения в разработке;
- научиться выявлять и анализировать распространённые уязвимости веб-приложений и системного уровня;
- сформировать навыки применения механизмов шифрования, хеширования и цифровой подписи;
- овладеть инструментами для оценки безопасности и тестирования приложений;
- развить умение проектировать архитектуру с учётом требований безопасности и оценки рисков.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

- основные принципы и методы обеспечения информационной безопасности программных систем;
- современные криптографические алгоритмы и их применение в разработке;
- распространённые типы уязвимостей и угроз для веб-приложений и системного уровня.

уметь:

- применять криптографические механизмы (шифрование, хеширование, цифровая подпись) в программных решениях;
- обнаруживать и анализировать типовые уязвимости в веб-приложениях и системах;
- использовать инструменты для оценки безопасности и тестирования приложений.

владеть:

— разрабатывать программное обеспечение с учётом требований безопасности;
— внедрять инструменты обнаружения уязвимостей в производственный процесс;
— формулировать и реализовывать базовые меры защиты информации на уровне архитектуры приложения и системы;
— оценивать риски, связанные с реализацией функциональности, и делать выбор в пользу безопасных решений.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
ОПК-1.	Способен находить, формулировать и решать актуальные и значимые проблемы прикладной и компьютерной математики	ОПК-1.1.	Знает основные методы и подходы к решению задач прикладной и компьютерной математики, включая алгоритмы, математическое моделирование и теорию оптимизации, а также современные инструменты и технологии, используемые в этой области
		ОПК-1.2.	Умеет анализировать и формулировать математические задачи, применять соответствующие методы и алгоритмы для их решения, а также интерпретировать и представлять результаты в понятной и доступной форме
		ОПК-1.3.	Имеет практический опыт работы над проектами или исследованиями в области прикладной и компьютерной математики, включая участие в конкурсах, олимпиадах или научных публикациях, где были решены актуальные и значимые задачи
ПК-1.	Способен определять общие формы и закономерности области управления командами разработки	ПК-1.1.	Знает основные теоретические концепции и принципы, относящиеся к области управления командами разработки, а также ключевые закономерности и модели, которые помогают в анализе и интерпретации данных
		ПК-1.2.	Умеет проводить систематический анализ области управления командами разработки, выявлять и формулировать общие закономерности и тенденции, а также применять методы исследования для получения новых знаний и понимания
		ПК-1.3.	Имеет практический опыт работы в области управления

			командами разработки, включая участие в научных проектах, исследованиях или практических заданиях, где были выявлены и описаны общие формы и закономерности
ПК-3.	Способен решать задачи профессиональной деятельности, формулировать результат, увидеть следствия полученного результата	ПК-3.1.	Знает основные принципы и методы решения задач профессиональной деятельности, а также способы формулирования и представления результатов, включая анализ последствий и их значимость в контексте проекта
		ПК-3.2.	Умеет применять математические и компьютерные методы для решения конкретных задач, формулировать четкие и обоснованные результаты, а также анализировать их последствия для дальнейших действий и решений
		ПК-3.3.	Имеет практический опыт в решении профессиональных задач, включая участие в проектах, где были получены результаты и проанализированы их следствия, что способствовало принятию обоснованных решений
ПК-5.	Способен передавать результат решенных прикладных задач в виде конкретных рекомендаций, выраженных в терминах области управления командами разработки	ПК-5.1.	Знает основные методы и подходы к формулированию рекомендаций на основе результатов решения прикладных задач, а также термины и концепции, специфичные для предметной области
		ПК-5.2.	Умеет анализировать результаты решенных задач и формулировать четкие, конкретные рекомендации, адаптируя их к требованиям и ожиданиям целевой аудитории
		ПК-5.3.	Имеет практический опыт в разработке и представлении рекомендаций на основе анализа прикладных задач, включая участие в проектах, где результаты были успешно применены и оценены в контексте предметной области

3. Тематический план

№ п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)			
1	Основные криптографические алгоритмы	7	7		40	Домашние задания
2	Безопасность на уровне операционной системы	7	7		40	Домашние задания Контест
3	Безопасность веб-приложений	3	3		20	Домашние задания Контест
4	Организационные аспекты информационной безопасности	7	7		40	Домашние задания Контест
	Зачет с оценкой			2		
	Итого:	***24***	***24***	***2***	***140***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основные криптографические алгоритмы	Основы криптографии. Генератор псевдослучайных чисел. Метод оценки эффективности ГПСЧ Сеть Фейстеля. Хэши. Коллизии хэшей и радужные таблицы. Блочные шифры. AES как пример блочного шифра. Асимметричное шифрование и цифровая подпись. Основы эллиптической криптографии
2	Безопасность на уровне операционной системы	Управление доступом в Linux. Пользователи и их права. DAC модель, ACL. PAM как средство аутентификации в систему. Механизм TOTP. Настройка аудита Изоляция в Linux. CGroups, Namespaces, Capabilities. Бинарные уязвимости и эксплуатация libc Безопасность Linux. Интерфейсы, туннели, firewall, теория PKI и работа сертификатов
3	Безопасность веб-приложений	Теория и практика Web уязвимостей. SQL injection, CSRF, path traversial, XSS Теория и практика Web уязвимостей. RCE, LFI, SSTI, IDOR, SSRF, DoS и Race Conditions
4	Организационные аспекты информационной безопасности	Протокол авторизации и аутентификации. Рассматриваем варианты на основе LDAP и KeyCloak. OIDC и OpenID Spring Security. Инфраструктура хранения секретов. Vault Основы контейнерной безопасности. Container Escapes

		Построение DevSecOps процессов, Vulnerability Management (управление уязвимостями), ASOC системы

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783.

2. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741.

Дополнительная литература:

1. Лось, А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов. — 2-е изд., испр. — Москва : Юрайт, 2025. — 424 с. — Текст : электронный

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;

— компьютерной техникой;

— механическими калькуляторами;

— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное

Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Информационная безопасность» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, домашние задания, контесты, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал, использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Контест – интерактивная платформа с заданиями разного уровня сложности и автоматической проверкой результатов.

Контест позволяет оперативно оценивать усвоение материала и выявлять пробелы в знаниях через тесты и практические задачи. Такой формат способствует регулярной

самопроверке и повышает мотивацию к изучению дисциплины.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Информационная безопасность»

Оценивание уровня учебных достижений обучающихся по дисциплине (модулю) осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой,*** при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	**Пятибалльная оценка**	**Общая характеристика результата обучения по дисциплине (модулю)**
10	Отлично	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину (модуль). Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
9	Отлично	
8	Отлично	
7	Хорошо	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими
6	Хорошо	

Десятибалльная оценка	Пятибалльная оценка	Общая характеристика результата обучения по дисциплине (модулю)
		задачами.
5	Удовлетворительно	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	
3	Не сдан	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	
1	Не сдан	

Дисциплина (модуль) «Информационная безопасность» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	40%	6	Набор задач по темам недели
Контетсы	30%	3	Интерактивные задания разного уровня сложности с автоматической проверкой результатов
Зачет с оценкой	30%	1	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

Формула расчёта итоговой оценки по дисциплине (модулю) «Информационная безопасность»: «0,4 × среднее за домашние задания + 0,4 × среднее за контесты + 0,6 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание 1: Криптографическая защита данных

1. Реализуйте модуль регистрации пользователя с хешированием пароля через алгоритм bcrypt или Argon2.
2. Напишите функцию шифрования файла алгоритмом AES-256 в режиме CBC с случайным вектором инициализации (IV).
3. Реализуйте проверку цифровой подписи сообщения с использованием асимметричного ключа RSA-2048.
4. Используйте CSPRNG для генерации криптографически стойких ключей и солей длиной не менее 256 бит.
5. Подготовьте отчёт с сравнением производительности хеш-функций (SHA-256 vs bcrypt) на больших объёмах данных.

Домашнее задание 2: Безопасность веб-приложений и ОС

1. Создайте REST-контроллер с эндпоинтами для загрузки и скачивания файлов пользователями.
2. Устраните уязвимость Path Traversal в методе скачивания файла с помощью валидации пути.
3. Настройте правила firewall (iptables/ufw) для блокировки всех входящих портов кроме SSH и HTTP.
4. Реализуйте защиту от CSRF-атак с использованием уникальных токенов для всех

POST-запросов.
5. Настройте аудит действий пользователя в Linux через демон auditd (логирование sudo и доступа к файлам).

Домашнее задание 3: DevSecOps и управление доступом

1. Разверните сервис HashiCorp Vault в Docker-контейнере для хранения секретов приложения.
2. Настройте получение секрета (пароля БД) приложением через API Vault при старте сервиса.
3. Напишите Dockerfile с использованием минимального базового образа (Alpine) и запуском от пользователя non-root.
4. Интегрируйте сканер уязвимостей (Trivy/Grype) в шаг сборки CI/CD пайплайна (GitLab CI/GitHub Actions).
5. Настройте единую точку входа (SSO) через Keycloak с использованием протокола OIDC для веб-приложения.

Примерные задания для контеста

Задание 1: Криптографический модуль защиты

Описание:

Разработайте модуль для безопасного хранения и передачи данных с использованием криптографических примитивов.

Шаги выполнения:

1. Напишите функцию хеширования пароля с использованием bcrypt (стоимость не менее 12).
2. Реализуйте генерацию криптографически стойкого ключа длиной 256 бит через CSPRNG.
3. Зашифруйте текстовое сообщение алгоритмом AES-256-GCM с случайным nonce.
4. Создайте функцию проверки цифровой подписи сообщения (RSA-2048 + SHA-256).
5. Подготовьте тесты, подтверждающие корректность шифрования/дешифрования.

Критерии автоматической проверки:

- Хеш пароля имеет корректный формат bcrypt (2*b*...).
- Длина ключа — ровно 32 байта (256 бит).
- Расшифрованное сообщение совпадает с исходным.
- Подпись проходит верификацию на тестовых данных.
- Все тесты завершаются статусом PASSED.

Флаг для сдачи:

Хеш зашифрованного файла в формате SHA-256 (hex).

Задание 2: Защита веб-приложения от уязвимостей

Описание:

Получите доступ к уязвимому веб-приложению (Docker-образ), найдите и устраните критические уязвимости.

Шаги выполнения:

1. Разверните локально предоставленный образ уязвимого приложения.
2. Найдите и эксплуатируйте SQL Injection в форме логина (получите список пользователей).
3. Исправьте уязвимость, внедрив параметризованные запросы в коде.
4. Добавьте защиту от XSS через экранирование вывода и заголовок Content-Security-Policy.
5. Реализуйте CSRF-токены для всех POST-запросов в приложении.

Критерии автоматической проверки:

- SQLMap не находит уязвимостей после исправления.
- Внедрение <script>alert(1)</script> не выполняется в браузере.
- POST-запрос без CSRF-токена возвращает ошибку 403.
- Сканер OWASP ZAP показывает уровень риска «Low» или «Clean».
- Приложение остаётся функциональным после всех изменений.

Флаг для сдачи:
Скриншот отчёта сканера уязвимостей со статусом «Clean».

Задание 3: DevSecOps пайплайн безопасности
Описание:
Настройте CI/CD пайплайн со встроенными проверками безопасности для контейнеризированного приложения.
Шаги выполнения:

1. Напишите Dockerfile с запуском от non-root пользователя (USER app).
2. Используйте минимальный базовый образ (Alpine или Distroless).
3. Добавьте этап сканирования уязвимостей через Trivy в CI/CD конфигурацию.
4. Настройте получение секрета из HashiCorp Vault при старте приложения.
5. Реализуйте блокировку пайплайна при обнаружении критических уязвимостей (CRITICAL/HIGH).

Критерии автоматической проверки:

- Контейнер не запускается от пользователя root (проверка через whoami).
- Сканирование Trivy завершается без критических уязвимостей.
- Секреты не хранятся в коде или логах пайплайна.
- Пайплайн автоматически падает при нахождении уязвимости CVE с уровнем Critical.
- Приложение успешно разворачивается и отвечает на health-check.

Флаг для сдачи:
Ссылка на успешный пайплайн с зелёным статусом и отчётом Trivy.

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1.	Как называется свойство хэш-функции, при котором сложно подобрать входные данные под заданное значение хэша?	устойчивость к прообразу (preimage resistance)	ОПК-1
2.	Какая криптографическая конструкция строится на раундовом преобразовании половин блока?	сеть Фейстеля (Feistel network)	ОПК-1
3.	Как называется генератор, предназначенный для получения криптографически стойких случайных чисел?	криптографически стойкий генератор псевдослучайных чисел (CSPRNG — Cryptographically Secure Pseudo-Random Number Generator)	ОПК-1
4.	Какой механизм подтверждает подлинность отправителя и целостность сообщения с использованием закрытого ключа?	цифровая подпись (Digital Signature)	ОПК-1

5.	Как называется список, определяющий права субъектов на объект в файловой системе?	список управления доступом (ACL — Access Control List)	ОПК-1
6.	Какая уязвимость позволяет выполнить произвольную команду на сервере через пользовательский ввод?	удалённое выполнение кода (RCE — Remote Code Execution)	ПК-1
7.	Как называется атака внедрения вредоносного сценария в веб-страницу, исполняемого в браузере?	межсайтовое выполнение сценариев (XSS — Cross-Site Scripting)	ПК-1
8.	Какой протокол используется для федеративной аутентификации поверх OAuth 2.0?	протокол открытой идентификации (OpenID Connect, OIDC)	ПК-1
9.	Как называется механизм одноразовых паролей, основанный на текущем времени?	одноразовый пароль на основе времени (TOTP — Time-Based One-Time Password)	ПК-1
10.	Какой тип атаки связан с подменой идентификатора ресурса для получения несанкционированного доступа?	небезопасная прямая ссылка на объект (IDOR — Insecure Direct Object Reference)	ПК-1
11.	Как называется процесс проверки защищённости системы путём моделирования атак?	тестирование на проникновение (penetration testing)	ПК-3
12.	Какой механизм Linux ограничивает потребление ресурсов процессами?	контрольные группы (cgroups — control groups)	ПК-3
13.	Как называется инфраструктура управления открытыми ключами и сертификатами?	инфраструктура открытых ключей (PKI — Public Key Infrastructure)	ПК-3
14.	Какой тип атаки использует предварительно вычисленные таблицы соответствия паролей и хэшей?	радужные таблицы (rainbow tables)	ПК-3
15.	Как называется внедрение SQL-кода через параметры запроса?	внедрение SQL-кода (SQL injection)	ПК-3
16.	Как называется процесс систематического выявления, оценки и устранения уязвимостей?	управление уязвимостями (Vulnerability Management)	ПК-5
17.	Как называется интеграция практик безопасности в процессы разработки и эксплуатации?	безопасная разработка и эксплуатация	ПК-5
18.	Как называется централизованная служба каталогов для хранения информации о пользователях и их правах?	протокол облегчённого доступа к каталогам (LDAP — Lightweight Directory Access Protocol)	ПК-5
19.	Как называется попытка вывести контейнер за пределы изолированной среды выполнения?	выход из контейнера (Container Escape)	ПК-5
20.	Как называется атака, направленная на исчерпание ресурсов сервиса с целью отказа в обслуживании?	отказ в обслуживании (DoS — Denial of Service)	ПК-5