ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

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

Рабочая программа дисциплины (модуля)
«Информационная безопасность»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Дизайн и разработка информационных продуктов*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 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)** 3
2. **Перечень планируемых результатов обучения** 5
3. **Тематический план** 5
4. **Содержание дисциплины (модуля)** 9
5. **Учебно-методическое обеспечение** 10
6. **Материально-техническое обеспечение** 10
7. **Методические и оценочные материалы** 12

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 02.03.01 Математика и компьютерные науки, профиль Дизайн и разработка информационных продуктов, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Информационная безопасность» позволяет будущим специалистам предотвращать уязвимости на ранних этапах, минимизируя риски и повышая устойчивость информационной инфраструктуры, в условиях роста киберугроз и цифровизации.

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 02.03.01 Математика и компьютерные науки, профиль Дизайн и разработка информационных продуктов и входит в обязательную часть Блока 1.

Дисциплина (модуль) изучается на 3 курсе в 6 семестре.

Цель изучения дисциплины (модуля): формирование у обучающихся системного понимания принципов и практик обеспечения безопасности информационных систем на всех этапах их жизненного цикла — от проектирования до эксплуатации.

Задачи изучения дисциплины (модуля):

- освоить модели угроз, включая STRIDE и аналоги, для анализа архитектуры систем и выявления потенциальных уязвимостей;
- изучить практические основы криптографии: применение хешей, цифровых подписей, TLS и управление криптографическими ключами;
- овладеть методами анализа и защиты веб-приложений и API на основе OWASP Top 10 и API Security Top 10;
- научиться реализовывать эффективные механизмы контроля доступа с использованием RBAC, ABAC и принципа минимальных привилегий;
- развить навыки реагирования на инциденты и безопасной эксплуатации систем, включая базовый security review и подготовку отчётов по рискам.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

- модели угроз и подходы к threat modeling (STRIDE и аналоги);
- основы криптографии на практике: хеши, подписи, TLS, управление ключами.
- безопасность веб-приложений и API (OWASP Top 10, API Security Top 10);
- контроль доступа: аутентификация/авторизация, RBAC/ABAC, принципы least privilege;
- основы реагирования на инциденты и безопасной эксплуатации;

уметь:

- выявлять угрозы и уязвимости по архитектуре и коду, предлагать меры защиты;
- настраивать безопасное хранение секретов и работать с токенами/сессиями;
- проводить базовый security review (инъекции, XSS, SSRF, десериализация, CSRF);

владеть:

- навыками безопасной разработки: чек-листы, линтеры/сканеры, угроз-модели как артефакт;

— навыками понимания компромиссов между безопасностью, удобством и скоростью разработки;
— навыками подготовки коротких отчётов по рискам и рекомендациям.

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)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области искусственного интеллекта, основные принципы критической оценки источников информации и их релевантности
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
УК-2.	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.	Знает действующие правовые нормы, регулирующие деятельность в области решения задач, основные методы и подходы к определению круга задач

		УК-2.2.	Умеет определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения задач, учитывая имеющиеся ресурсы и ограничения
		УК-2.3.	Имеет практический опыт применения знаний о правовых нормах и ресурсах в реальных ситуациях, разработки и реализации решений в соответствии с установленными ограничениями
ОПК-1.	Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности	ОПК-1.1.	Знает основные концепции и теории в области математического анализа и смежных дисциплин; методы и подходы, используемые в различных областях математики
		ОПК-1.2.	Умеет применять математические методы для решения профессиональных задач
		ОПК-1.3.	Имеет практический опыт разработки и реализация математических моделей в профессиональной деятельности
ОПК-5.	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-5.1.	Знает технологии, необходимые для прикладного программирования, включая современные функциональные языки программирования, а также основные принципы и понятия, применяемые при использовании

			компьютерных сетей
		ОПК-5.2.	Умеет пользоваться технологиями прикладного программирования, включая среды высокоуровневого программирования
		ОПК-5.3.	Имеет практический опыт использования технологий прикладного программирования
ПК-1.	Способен формулировать задачи с математической точностью, обосновывать утверждения строго и анализировать полученные результаты в области математики и компьютерных наук	ПК-1.1.	Знает методы и подходы к формулированию задач, а также основные принципы математического доказательства и анализа результатов
		ПК-1.2.	Умеет корректно ставить и формулировать математические задачи, применять строгие методы доказательства и анализировать полученные результаты
		ПК-1.3.	Имеет опыт работы с задачами в области математики и компьютерных наук, включая применение математических методов для решения практических задач
ПК-2.	Способен решать типовые задачи профессиональной деятельности, опираясь на информационную и библиографическую культуру, используя информационно-коммуникационные технологии и учитывая основные требования информационной безопасности	ПК-2.1.	Знает основы информационной и библиографической культуры, а также принципы информационной безопасности и применения информационно-коммуникационных технологий в профессиональной деятельности

		ПК-2.2.	Умеет эффективно использовать информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности, учитывая требования информационной безопасности
		ПК-2.3.	Имеет опыт работы с информационными ресурсами и технологиями в области профессиональной деятельности, включая соблюдение норм информационной безопасности
ПК-4.	Способен разрабатывать программное обеспечение для решения прикладных задач в области профессиональной деятельности под руководством более опытного специалиста	ПК-4.1.	Знает основные принципы разработки программного обеспечения и методы решения прикладных задач в сфере профессиональной деятельности
		ПК-4.2.	Умеет разрабатывать программное обеспечение под руководством специалистов более высокой категории, используя современные технологии и инструменты
		ПК-4.3.	Имеет опыт участия в разработке программного обеспечения для решения прикладных задач в команде под руководством более опытных специалистов

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы					ТКУ (текущий контроль успеваемости)
		Очная форма					
		Контактная работа			Контроль	Самостоятельная работа	
		Лекции	Семинары (практические занятия)	Консультации			
1	Введение	2	2	1		11	Домашние задания
2	Threat modeling	2	2	1		11	Домашние задания
3	Криптография на практике	2	2	1	6	11	Домашние задания Коллоквиум
4	Контроль доступа	2	2	1		11	Домашние задания
5	OWASP практики	3	3	1		12	Домашние задания
6	Безопасность инфраструктуры	3	3	1		12	Домашние задания
7	Безопасность API	3	3	2		12	Домашние задания
8	Защита данных	3	3	2		12	Домашние задания
9	Secure SDLC	3	3	2		12	Домашние задания
10	Инциденты	3	3	2		12	Мини-проект
	Экзамен				2		
Итого:		***26***	***26***	***14***	***8***	***116***	
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	Введение	Модель атакующего, поверхности атаки, безопасность по умолчанию
2	Threat modeling	STRIDE, data flow diagrams, приоритизация рисков
3	Криптография на практике	Хеши, подписи, TLS, секреты, key management
4	Контроль доступа	Аутентификация/авторизация, токены, RBAC/ABAC
5	OWASP практики	Инъекции, XSS/CSRF, SSRF, небезопасная десериализация
6	Безопасность инфраструктуры	Секреты, конфиги, минимальные права, аудит
7	Безопасность API	Версионирование, ошибки, rate limiting, защита от abuse
8	Защита данных	PII, шифрование, политики хранения, логирование без утечек
9	Secure SDLC	Code review, SAST/DAST, dependency scanning, SBOM
10	Инциденты	Логи, расследование, ротация ключей, коммуникация

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. Безопасность веб-приложений. Разведка, защита, нападение - СПб:Питер, 2022: ISBN. - Текст : электронный. - URL: https://znanium.com/catalog/product/2125433.

2. Фленов, М. Е. Linux глазами хакера : практическое руководство / М. Е. Фленов. - 6-е изд., перераб. и доп. - Санкт-Петербург : БХВ-Петербург, 2021. - 416 с. - ISBN 978-5-9775-6699-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2139146.

3. Скабцов, Н. Аудит безопасности информационных систем : практическое руководство / Н. Скабцов. - Санкт-Петербург : Питер, 2018. - 272 с. - (Серия «Библиотека программиста»). - ISBN 978-5-4461-0662-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1760857.

Дополнительная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560426.

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, коллоквиумы, домашние задания, 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.

Консультации – структурированные встречи, на которых преподаватели предоставляют индивидуальную или групповую помощь в освоении учебного материала, обсуждении вопросов и решении проблем, возникающих в процессе обучения.

Консультации могут включать разъяснение сложных тем, подготовку к экзаменам и помощь в выполнении проектных работ, что способствует более глубокому пониманию предмета и улучшению академической успеваемости.

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.

Коллоквиум – устные ответы на вопросы, список которых известен студенту заранее.

В процессе подготовки к коллоквиуму необходимо проанализировать учебные материалы, ознакомившись с лекциями, учебниками и дополнительными источниками, акцентируя внимание на ключевых темах. Рекомендуется создать структурированные конспекты, выделяя основные идеи, термины и формулы.

Мини-проект — это краткосрочная практическая работа в малых группах на семинарах, направленная на применение теоретических знаний для решения конкретных задач.

В ходе мини-проекта студенты проводят анализ проблемы, разрабатывают техническое решение и представляют результаты в виде отчета, модели или презентации. Такой формат способствует развитию навыков самостоятельной работы, критического мышления и командного взаимодействия.

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 ***экзамена***, 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:

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. 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,
9	Отлично	
8	Отлично	

Десятибалльная оценка	Пятибалльная оценка	Общая характеристика результата обучения по дисциплине (модулю)
		необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
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 задачами.
6	Хорошо	
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	20%	8	Набор задач по темам недели
Коллоквиум	20%	1	Письменная работа с набором задач, которые нужно решить за ограниченное время
Мини-проект	30%	1	Краткосрочная практическая работа в малых группах на семинарах, направленная на применение теоретических знаний для решения конкретных задач.
Экзамен	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»: «0,2 × среднее за домашние задания + 0,2 × коллоквиум + 0,3 × мини-проект + 0,3 × экзамен».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание по теме «Threat modeling».

Постройте диаграмму потоков данных (DFD) для простого API-сервиса аутентификации, примените модель STRIDE для выявления минимум 6 угроз, классифицируйте их по уровню риска (например, по матрице вероятность × ущерб) и предложите по одной мере защиты для каждой критической угрозы.

Домашнее задание по теме «Криптография на практике».

Реализуйте безопасное хранение паролей с использованием хеширования (например, bcrypt), подпишите тестовое сообщение с помощью цифровой подписи (RSA или ECDSA), настройте локальный HTTPS-сервер с валидным сертификатом (например, через mkcert) и опишите стратегию управления секретами (ключи API, пароли БД) в среде разработки и продакшене.

Домашнее задание по теме «Безопасность API».

Разработайте REST API с версионированием (например, **/v1/users**), реализуйте обработку ошибок без раскрытия внутренней информации, настройте rate limiting (например, 100 запросов в минуту на IP) и добавьте защиту от массовых запросов (например, через middleware). Обоснуйте, как эти меры защищают от злоупотреблений.

Домашнее задание по теме «Secure SDLC».

Проведите ручной security code review небольшого open-source проекта (или предложенного преподавателем), запустите SAST-сканер (например, Semgrep или Bandit), проверьте зависимости на уязвимости (с помощью **npm audit** или **pip-audit**), сгенерируйте SBOM (Software Bill of Materials) и оформите отчёт с найденными рисками и рекомендациями.

Примерные вопросы для коллоквиума.

1. Что входит в понятие «поверхность атаки»? Приведите примеры её компонентов для веб-приложения и объясните, как её можно сократить.
2. Как модель STRIDE помогает при анализе угроз? Примените её к одному из компонентов диаграммы потоков данных (например, хранилищу данных).
3. В чём разница между хешированием и шифрованием? Почему для хранения паролей нельзя использовать MD5 или SHA-1?
4. Объясните разницу между RBAC и ABAC. В каких случаях ABAC предпочтительнее?
5. Как работает атака XSS? Какие меры защиты эффективны против отражённого и хранимого XSS?
6. Почему важно запускать приложения с минимальными привилегиями? Приведите пример из практики (например, Docker или ОС).
7. Как rate limiting и версионирование API способствуют его безопасности? Что может

произойти при их отсутствии?

8. Что такое PII и как его следует обрабатывать при логировании? Приведите пример утечки через логи и способы её предотвращения.
9. Для чего нужен SBOM? Как он помогает в управлении уязвимостями в зависимостях?
10. Опишите типичные шаги при реагировании на инцидент утечки API-ключа. Почему важна ротация секретов и как её организовать?

Примеры заданий и критерии оценивания мини-проекта.

Описание:

Ваша команда (2–3 человека) получает архитектурное описание и фрагмент кода простого веб-приложения — сервиса управления задачами (аналог Trello/ToDo). Приложение включает:

— Регистрацию и аутентификацию пользователей
— Создание, редактирование и удаление задач
— REST API для взаимодействия с фронтендом
— Хранение данных в базе данных
— Работу в Docker-контейнере

Задача:

Проведите комплексный анализ безопасности приложения и предложите меры по его защите, охватывая все ключевые аспекты курса. Результат представьте в виде **краткого отчёта (3–5 страниц)** или **презентации (8–10 слайдов)**.

Шаги выполнения:

1. Постройте **диаграмму потоков данных (DFD)** и определите **поверхность атаки** .
2. Проведите **threat modeling** с использованием STRIDE: выявите минимум 5 угроз и приоритизируйте их.
3. Укажите, как реализованы (или должны быть реализованы):
   — Хеширование паролей и управление секретами
   — Аутентификация (токены, сессии) и контроль доступа (RBAC/ABAC)
   — Защита от OWASP Top 10 (инъекции, XSS, CSRF и др.)
4. Оцените безопасность инфраструктуры: запуск от непривилегированного пользователя, конфигурация, логирование.
5. Предложите меры по защите API: версионирование, rate limiting, обработка ошибок.
6. Опишите, как обрабатываются PII, где применяется шифрование, как настроены политики хранения и логирования.
7. Добавьте в отчёт элементы Secure SDLC: предложите чек-лист для code review, укажите, какие SAST/DAST-инструменты можно использовать, и сгенерируйте пример SBOM (можно условно).
8. Разработайте план реагирования на инцидент: что делать при утечке API-ключа (ротация, аудит, коммуникация).

Формат представления: Отчёт или презентация с кратким устным выступлением (5–7 минут) на семинаре.

Критерии оценивания участия студентов в мини-проекте

— Полнота охвата тем безопасности: Проект охватывает все ключевые аспекты, указанные в задании (от threat modeling до реагирования на инциденты), демонстрируя

системный подход к защите приложения;

— Глубина анализа и техническая корректность: Предложенные решения основаны на актуальных практиках информационной безопасности, используются правильные термины и технологии (например, bcrypt, JWT, rate limiting), угрозы обоснованы и реалистичны;

— Практическая применимость решений: Меры защиты не носят абстрактный характер, а могут быть реализованы в реальной системе; предложены конкретные инструменты, настройки или кодовые примеры;

— Качество оформления и структурированность материала: Отчёт или презентация логичны, содержат чёткую структуру, визуализации (DFD, таблицы угроз), легко воспринимаются и отражают суть проведённой работы;

— Навыки командной работы и распределение ролей: Члены команды эффективно взаимодействуют, вклад каждого прослеживается, при защите проекта оба участника активно участвуют в презентации и ответах на вопросы.

— Критическое мышление и обоснование решений: Студенты осознают компромиссы (например, между безопасностью и удобством), могут объяснить, почему выбран тот или иной подход, а не просто перечислить рекомендации;

— Активность и вовлечённость в процесс: Проявляется интерес к задаче, инициатива в поиске решений, готовность уточнять и улучшать работу в ходе обсуждения с преподавателем или другими группами.

Задачи и этапы выполнения проекта:

— Выбор и описание приложения.

Разработать или выбрать существующее Java-приложение (многопоточное, с нетривиальной логикой и измеримой нагрузкой), описать его архитектуру, сценарии использования и ожидаемые характеристики (latency, throughput, footprint).

— Анализ исполнения на уровне JVM.

Исследовать процесс компиляции и выполнения программы: проанализировать структуру скомпилированных class-файлов и байткода (например, с использованием javap), описать модель вызовов методов, особенности загрузки классов и динамики типов.

— Исследование производительности и JIT.

Провести измерения производительности с учетом прогрева JVM, проанализировать влияние tiered compilation и JIT-оптимизаций, выявить «горячие» участки кода (hot paths) и объяснить наблюдаемое поведение с точки зрения рантайма и возможной деоптимизации.

— Анализ памяти и сборки мусора.

Исследовать аллокации объектов, особенности layout, поведение GC (тип сборщика, частота, паузы STW), оценить влияние выбранных структур данных и алгоритмов на потребление памяти и производительность.

— Анализ многопоточности и корректности.

Проанализировать многопоточные участки программы с позиции Java Memory Model: обосновать корректность синхронизации, проверить отсутствие гонок данных и объяснить гарантии happens-before.

— Оптимизация и инженерное обоснование решений.

Предложить и реализовать улучшения (в коде, конфигурации JVM или архитектуре), провести повторные измерения и аргументированно оценить компромиссы (производительность, задержки, потребление памяти, сложность поддержки).

— Подготовка отчета.

Представить результаты в виде структурированного отчета с описанием гипотез, методики экспериментов, полученных данных, интерпретации результатов и итоговых выводов.

Критерии оценивания.

1. Глубина технического анализа — корректность и полнота объяснения поведения программы на уровне JVM (байткод, JIT, GC, загрузка классов, JMM), а не только на уровне исходного кода.
2. Обоснованность экспериментальной методики — наличие воспроизводимых измерений, корректный учет прогрева JVM, использование инструментов профилирования и диагностики.
3. Качество инженерной аргументации — способность формулировать гипотезы, интерпретировать результаты и обосновывать выбор оптимизаций с учетом платформенных компромиссов.
4. Корректность анализа многопоточности — грамотное применение принципов Java Memory Model и аргументированная оценка наличия или отсутствия гонок данных.
5. Целостность и профессиональный уровень представления работы — логичность структуры отчета, ясность выводов, использование технической терминологии и наглядных материалов (графиков, профилей, фрагментов байткода).

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1	Назовите модель, описывающую возможные действия злоумышленника в системе.	модель атакующего	УК-1
2	Укажите метод визуализации архитектуры, применяемый при анализе угроз.	диаграмма потоков данных	УК-1
3	Что является основой подхода, при котором система остаётся безопасной даже при компрометации одного компонента?	принцип устойчивости	УК-1
4	Укажите механизм, предотвращающий выполнение действий от имени пользователя без его ведома.	CSRF-токен	УК-2
5	Что используется для подтверждения личности с помощью пароля и одноразового кода?	двухфакторная аутентификация	УК-2
6	Определите понятие, при котором доступ зависит от атрибутов пользователя, ресурса и времени.	ABAC	УК-2
7	Вставьте название алгоритма, рекомендуемого для хеширования паролей с солью.	bcrypt	ОПК-1
8	Что описывает свойство хеш-функции, при котором невозможно восстановить вход по выходу?	однонаправленность	ОПК-1
9	Что применяется для установления защищённого канала между веб-браузером и сервером?	асимметричное шифрование	ОПК-1
10	Укажите протокол, обеспечивающий шифрование и целостность данных в HTTP-трафике.	TLS	ОПК-5

11	Что используется для передачи информации о правах между микросервисами в закодированной форме?	JWT	ОПК-5
12	Что предотвращает перегрузку API из-за множества запросов от одного IP-адреса?	rate limiting	ОПК-5
13	Укажите тип уязвимости, возникающей при вставке непроверенного ввода в SQL-запрос.	инъекция	ПК-1
14	Что применяется для анализа исходного кода на уязвимости без его выполнения?	SAST	ПК-1
15	Что защищает от выполнения вредоносного кода при десериализации объектов?	валидация данных	ПК-1
16	Дайте определение журналу, фиксирующему все действия пользователей в системе.	аудит	ПК-2
17	Что используется для автоматического поиска уязвимых библиотек в проекте?	сканер зависимостей	ПК-2
18	Что предотвращает утечку персональных данных через логи приложения?	маскировка PII	ПК-2
19	Укажите название документа, перечисляющего все компоненты программного обеспечения.	SBOM	ПК-4
20	Что является безопасным способом хранения API-ключей в облачной инфраструктуре?	менеджер секретов	ПК-4
21	Что применяется для шифрования данных при хранении в базе с использованием одного ключа?	симметричное шифрование	ПК-4