

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Тольяттинский государственный университет»

Б1.О.21  
(индекс дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Обеспечение безопасности при разработке программного обеспечения**  
(наименование дисциплины)

по направлению подготовки

09.03.03 Прикладная информатика  
направленность (профиль)

Автоматизация бизнес-процессов и проектирование ИТ-решений

Форма обучения: заочная

Год набора: 2024

Общая трудоемкость: 5 ЗЕ

**Распределение часов дисциплины по семестрам**

Семестр	5	Итого
Форма контроля	экзамен	
Вид занятий		
Лекции	4	4
Лабораторные		
Практические		
ККР	1	1
Промежуточная аттестация	0,35	0,35
Контактная работа	5,35	5,35
Самостоятельная работа	166	166
Контроль	8,65	8,65
<b>Итого</b>	<b>180</b>	<b>180</b>

Рабочую программу составила:

Доцент института цифровых технологий, к.э.к.наук, Раченко Т.А.

---

*(должность, ученое звание, степень, Фамилия И.О.)*

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

---

*(должность, ученое звание, степень, Фамилия И.О.)*

Рабочая программа составлена на основании ФГОС ВО и учебного плана направления подготовки

09.03.03 Прикладная информатика

---

*(код и наименование направления подготовки, специальности в соответствии с ФГОС ВПО)*

**Срок действия рабочей программы дисциплины до «31» августа 2031 г.**

УТВЕРЖДЕНО

На заседании института цифровых технологий

---

(протокол заседания № 1 от «05» сентября 2025 г.)

## **1. Цель освоения дисциплины**

Цель – формирование у обучающихся компетенций в области обеспечения безопасности при разработке программного обеспечения, в том числе для систем искусственного интеллекта и обработки больших данных, включая методы защиты данных, моделей и конвейеров машинного обучения.

Задачи:

1. Изучение типовых уязвимостей программного обеспечения и методов их предотвращения, с акцентом на уязвимости в системах ИИ и больших данных.
2. Знакомство с принципами проектирования безопасного программного обеспечения, включая защиту данных на всех этапах жизненного цикла.
3. Изучение методов и средств аутентификации и авторизации пользователей в распределённых системах обработки данных.
4. Знакомство с криптографическими методами и средствами защиты данных, включая гомоморфное шифрование и дифференциальную приватность.
5. Изучение протоколов безопасной передачи данных и методов защиты данных при передаче в облачные и распределённые хранилища.
6. Изучение методов обеспечения целостности данных, в том числе для наборов данных, используемых в обучении моделей.
7. Освоение навыков использования инструментальных средств обеспечения безопасности программного обеспечения, включая инструменты для анализа безопасности данных и моделей ML.
8. Формирование умения анализировать уязвимости программного обеспечения и разрабатывать политику информационной безопасности для проектов в области ИИ и больших данных.
9. Овладение приемами предотвращения, обнаружения и нейтрализации угроз безопасности программных систем, включая атаки на модели машинного обучения (отравление данных, инверсия моделей, атаки с подбором выходных данных).

## **2. Место дисциплины (учебного курса) в структуре ОПОП ВО**

Данная дисциплина (учебный курс) относится к блоку Б - обязательная часть.

Дисциплины, учебные курсы, на освоении которых базируется данная дисциплина (учебный курс) – Информационные системы и технологии, Управление проектами разработки программного обеспечения, Базы данных и управление данными, Обеспечение качества кода и код ревью.

Дисциплины, учебные курсы, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины (учебного курса) – Выполнение и защита выпускной квалификационной работы.

### 3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые 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 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности с использованием ИКТ и с учётом требований информационной безопасности.
	ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Уметь: применять ИКТ и методы обеспечения информационной безопасности при решении стандартных профессиональных задач.
	ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Владеть: навыками работы с информационными ресурсами и средствами защиты информации при решении профессиональных задач.
ОПК-5 Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.1 Знает принципы установки программного и аппаратного обеспечения для информационных и автоматизированных систем	Знать: принципы установки и настройки программного и аппаратного обеспечения информационных систем.
	ОПК-5.2 Умеет выполнять настройку информационных и автоматизированных систем	Уметь: выполнять установку и настройку программных и аппаратных средств с учётом требований безопасности.

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	ОПК-5.3 Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем	Владеть: навыками инсталляции, настройки и тестирования программного и аппаратного обеспечения для автоматизированных систем.

#### 4. Структура и содержание дисциплины Обеспечение безопасности при разработке программного обеспечения

Модуль (раздел)	Вид учебной работы	Наименование тем занятий	Курс	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
<b>1. Основы безопасности ПО и управление данными</b>	Лекция 1 (установочная)	Тема 1. Введение в безопасность при разработке программного обеспечения. Особенности безопасности систем ИИ и больших данных. Тема 1.1. Методы оптимизации управления жизненным циклом распределённых данных с учётом информационной безопасности. Приватность данных и дифференциальная приватность.	5	2	–	–	–
	Самостоятельная работа	1.1. Изучение основных понятий и терминологии (угрозы, уязвимости, риски, атаки). Классификация угроз (по источникам, по объектам воздействия).	5	12	–	–	–
	Самостоятельная работа	1.2. Анализ нормативно-правовой базы (ФЗ-149, ФЗ-152, приказы ФСТЭК). Обзор международных стандартов ISO/IEC 27001, ISO/IEC 27034.	5	16	–	–	–
	Самостоятельная работа	1.3. Обзор методологий и подходов: OWASP Top 10, STRIDE, DREAD, Microsoft SDL.	5	14	–	–	–
	Самостоятельная работа	1.4. Изучение типовых уязвимостей: OWASP Top 10 для веб-приложений, CWE Top 25; практическое ознакомление с базами уязвимостей (CVE, NVD).	5	16	–	–	–
	Самостоятельная работа	Подготовка к ККР	5	28	–	–	–
	<b>Контрольная работа (ККР)</b>	Письменный опрос по модулю 1	5	1	15	–	ККР

Модуль (раздел)	Вид учебной работы	Наименование тем занятий	Курс	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
<b>2. Безопасность в сетевых технологиях и системах ИИ</b>	Лекция 2 (установочная)	Тема 2. Принципы информационной безопасности. Проектирование безопасности для систем сбора и обработки больших данных. Тема 3. Технология осуществления оптимизации управления жизненным циклом данных. Безопасность конвейеров обработки данных. Тема 4. Инструменты обеспечения безопасности на этапе разработки. Инструменты для анализа безопасности данных и моделей (TensorFlow Privacy, Adversarial Robustness Toolbox и др.).	5	2	–	–	–
	Самостоятельная работа (практическая работа №1)	<b>Практическая работа №1.</b> Разработка веб-приложения с функцией редактирования заметок и обеспечение базовой безопасности (Flask, защита от CSRF, IDOR).	5	12	6	–	Отчёт по работе (защита)
	Самостоятельная работа (практическая работа №2)	<b>Практическая работа №2.</b> Статический анализ кода и устранение уязвимостей (Bandit). Применение к коду, работающему с данными для обучения моделей.	5	12	5	–	Отчёт по работе (защита)
	Самостоятельная работа (практическая работа №3)	<b>Практическая работа №3.</b> Динамическое тестирование (DAST) и защита от OWASP Top 10 (OWASP ZAP). Проверка уязвимостей в приложениях, загружающих данные из внешних источников.	5	12	7	–	Отчёт по работе (защита)
	Самостоятельная работа (практическая работа №4)	<b>Практическая работа №4.</b> Защита от SQL-инъекций и тестирование с помощью SQLMap. Применение к базам данных, используемым для хранения признаков наборов.	5	12	7	–	Отчёт по работе (защита)

Модуль (раздел)	Вид учебной работы	Наименование тем занятий	Курс	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
	Самостоятельная работа (практическая работа №5)	<b>Практическая работа №5.</b> Обеспечение безопасности базы данных PostgreSQL. Настройка прав доступа и шифрования для хранилища данных, содержащего персональные данные.	5	12	6	–	Отчёт по работе (защита)
	Самостоятельная работа (практическая работа №6)	<b>Практическая работа №6.</b> Разработка плана безопасности и DevSecOps-интеграция. Включение проверок безопасности данных и моделей в CI/CD.	5	12	7	–	Отчёт по работе (защита)
	Самостоятельная работа (практическая работа №7)	<b>Практическая работа №7.</b> Мониторинг безопасности и реагирование на инциденты (SIEM Lite). Отслеживание аномалий в доступе к данным и работе моделей.	5	12	7	–	Отчёт по работе (защита)
	Самостоятельная работа	Подготовка к экзамену (систематизация материала, повторение ключевых вопросов)	5	28	–	–	–
<b>Контактная работа</b>				5,35	–	–	
<b>Самостоятельная работа</b>				166	–	–	
<b>Контроль</b>		Итоговый тест (экзамен)		8,65	40	–	
<b>Итого</b>				<b>180</b>	<b>100</b>	–	

#### Схема расчета итогового балла:

Текущий рейтинг (сумма баллов за ККР + практические работы) + результат итогового теста. Полученная сумма делится на 2. Максимальный итоговый балл – 100.



## **5. Образовательные технологии**

В рамках учебного курса предусмотрены следующие образовательные технологии:

- технология дистанционного обучения: лекции, практические занятия, самостоятельная работа, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и преподавателя.

## **6. Методические указания по освоению дисциплины**

Дистанционное обучение предполагает самостоятельное изучение учебных дисциплин с использованием электронных учебно-методических комплексов, размещенных в системе обучения, консультации преподавателя при подготовке к тестированию и по его итогам, при подготовке к зачетам и экзаменам, контрольных и курсовых работ, а также участие в электронных семинарах и практических занятиях.

Самостоятельная работа обучающихся проводится с целью углубления и расширения теоретических знаний; развития познавательных способностей и активности обучающихся; самостоятельности, ответственности и организованности, творческой инициативы; формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации.

Контроль выполненной самостоятельной работы осуществляется индивидуально, при защите рефератов, курсовых работ, творческих проектов, с использованием информационно - телекоммуникационных технологий.

### **6.1. Рекомендации по подготовке к лекционным занятиям**

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет.

В ходе лекционных занятий обучающимся необходимо изучить наиболее значимые и актуальные темы и вопросы учебной дисциплины. Помимо лекционного материала обучающимся также рекомендуется самостоятельно проработать каждую тему с использованием дополнительной учебной литературы, указанной в библиографии курса (дисциплины). Обучающийся может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и выпускных квалификационных работ.

После изучения лекционного материала обучающийся переходит к тестовому материалу, который состоит из тестов текущего контроля. Тесты текущего контроля размещены в конце каждой темы. К текущему тестированию обучающемуся рекомендуется готовиться по вопросам для самоподготовки. Текущее тестирование, прежде всего, является одним из элементов самоконтроля и закрепления обучающимся пройденного учебного материала.

### **6.2. Рекомендации по подготовке к практическим занятиям**

Практические занятия у дистанционных обучающихся могут проходить либо в виде тестирования, либо в виде практикума по решению задач.

Обучающимся следует:

- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и другие источники;
- во время выполнения заданий обучающийся может задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения, используя возможности форума, открытого в курсе системы обучения.

Доводить задания практической работы до окончательного решения, прикрепить выполненные задания в курсе системы обучения, в случае затруднений обращаться к преподавателю.

Форум – средство общения пользователей в сети с использованием специального программного обеспечения, позволяющее его участникам общаться между собой не в режиме реального времени. Сообщения, отправленные на форум, могут храниться в нём неограниченно долго, и ответ на форуме может быть дан в любое время, удобное его участнику, а не в тот же день, когда появился обсуждаемый вопрос. Посредством форума предоставляется возможность в системе дистанционного образования коллективного общения и обсуждения.

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по рассмотренному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса.

При этих условиях обучающийся не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул для активной проработки лекции.

### **6.3. Рекомендации по подготовке к экзамену**

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, обучающийся ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На зачете обучающийся демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

После изучения лекционного материала обучающийся переходит к тестовому материалу, который состоит из тестов промежуточной аттестации (зачет, экзамен).

Перед тестированием в формате переписки обучающийся имеет возможность получить консультацию преподавателя по наиболее сложным для него вопросам, а по итогам тестирования – оценку преподавателя и анализ уровня усвоения материала темы.

Тесты промежуточной аттестации произвольно формируются из вопросов по всем темам учебной дисциплины. Это позволяет преподавателю получить объективную оценку уровня знаний, умений и навыков, освоенных обучающимся.

Необходимо ориентировать обучающихся на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

## **7. Оценочные средства**

### **7.1 Паспорт оценочных средств экзамену**

<b>Семестр</b>	<b>Код контролируемой компетенции (или ее части)</b>	<b>Наименование оценочного средства</b>
5	ОПК-3; ОПК-5	Контрольная работа (ККР) Тестовые задания (экзамен) Вопросы к экзамену Отчеты по практическим работам №1–7

### **7.2 Типовые задания или иные материалы, необходимые для текущего контроля**

#### **7.2.1 Вопросы для собеседования по модулю**

## **Типовые примеры заданий**

### **Модуль 1. Основные понятия и определения безопасности информации. Требования безопасности разработки программного обеспечения**

1. Какие основные понятия и определения безопасности информации необходимо знать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
2. Какие требования безопасности необходимо учитывать при разработке программного обеспечения, и как они связаны с оптимизацией управления жизненным циклом распределенных данных?
3. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
4. Какие риски связанные с безопасностью данных могут возникнуть при разработке программного обеспечения, и как их можно предотвратить?
5. Какие принципы информационной безопасности необходимо учитывать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
6. Какие методы обеспечения безопасности данных можно использовать при разработке программного обеспечения, и как они связаны с управлением жизненным циклом распределенных данных?
7. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке программного обеспечения, и как они связаны с безопасностью информации?
8. Как оценить уровень безопасности разработанного программного обеспечения, и какие методы использовать для его улучшения?
9. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных вы можете порекомендовать обучающимся при разработке программного обеспечения?
10. Какие методы обнаружения и предотвращения уязвимостей в программном обеспечении существуют, и как они связаны с безопасностью данных и управлением жизненным циклом распределенных данных?
11. Какие методы защиты данных можно использовать при работе с базами данных, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
12. Какие методы защиты данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
13. Какие методы защиты данных можно использовать при работе с виртуальными частными сетями (VPN), и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
14. Какие методы обеспечения безопасности данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?
15. Какие методы обеспечения безопасности данных можно использовать при работе с веб-серверами, и как они связаны с управлением жизненным циклом распределенных данных и безопасностью информации?

### **Модуль 2. Сетевые технологии и информационная безопасность**

1. Какие принципы информационной безопасности необходимо учитывать при работе с сетевыми технологиями, и как они связаны с управлением жизненным циклом распределенных данных?

2. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
3. Какие риски связанные с безопасностью данных могут возникнуть при работе с сетевыми технологиями, и как их можно предотвратить?
4. Какие методы обеспечения безопасности данных можно использовать при работе с сетевыми технологиями, и как они связаны с управлением жизненным циклом распределенных данных?
5. Какие принципы управления жизненным циклом распределенных данных необходимо учитывать для обеспечения безопасности информации при работе с сетевыми технологиями?
6. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных для обеспечения безопасности информации вы можете порекомендовать обучающимся?
7. Какие методы защиты данных можно использовать при работе с беспроводными сетями, и как они связаны с управлением жизненным циклом распределенных данных?
8. Какие методы обеспечения безопасности данных можно использовать при работе с сетевыми протоколами, и как они связаны с управлением жизненным циклом распределенных данных?
9. Какие методы защиты данных можно использовать при работе с веб-серверами, и как они связаны с управлением жизненным циклом распределенных данных?
10. Какие принципы информационной безопасности следует учитывать при разработке сетевых приложений, и как они связаны с управлением жизненным циклом распределенных данных?
11. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при разработке сетевых приложений, и какие принципы безопасности данных следует учитывать?
12. Какие методы защиты данных можно использовать при работе с базами данных, и как они связаны с управлением жизненным циклом распределенных данных?
13. Какие методы защиты данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных?
14. Какие методы защиты данных можно использовать при работе с виртуальными частными сетями (VPN), и как они связаны с управлением жизненным циклом распределенных данных?
15. Какие методы обеспечения безопасности данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных?

### **Модуль 3. Разработка прикладных задач с учетом требований безопасности**

1. Какие методы оптимизации управления жизненным циклом распределенных данных существуют, и какие из них наиболее эффективны с точки зрения безопасности информации?
2. Какие риски связанные с безопасностью данных могут возникнуть при разработке прикладных задач, и как их можно предотвратить?
3. Какие принципы информационной безопасности необходимо учитывать при разработке прикладных задач, и как они могут быть реализованы?
4. Какие методы обеспечения безопасности данных можно использовать при разработке прикладных задач?
5. Какие принципы управления жизненным циклом распределенных данных необходимо учитывать для обеспечения безопасности информации?

6. Какие методы выбора оптимального метода управления жизненным циклом распределенных данных вы можете порекомендовать обучающимся?
7. Какие принципы информационной безопасности следует учитывать при разработке приложений для мобильных устройств, и как это связано с управлением жизненным циклом распределенных данных?
8. Какие риски связанные с безопасностью данных могут возникнуть при использовании облачных сервисов, и как их можно предотвратить?
9. Какие методы обеспечения безопасности данных можно использовать при работе с облачными сервисами, и как они связаны с управлением жизненным циклом распределенных данных?
10. Какие принципы управления жизненным циклом распределенных данных следует учитывать при разработке систем электронного документооборота, и как они связаны с безопасностью информации?
11. Какие методы оптимизации управления жизненным циклом распределенных данных можно использовать при работе с системами управления проектами, и какие принципы безопасности данных следует учитывать?
12. Какие методы защиты данных можно использовать при работе с мобильными приложениями, и как они связаны с управлением жизненным циклом распределенных данных?
13. Какие методы обеспечения безопасности данных можно использовать для защиты от кибератак, и как они связаны с управлением жизненным циклом распределенных данных?
14. Какие методы защиты данных можно использовать при работе с системами управления контентом, и как они связаны с управлением жизненным циклом распределенных данных?
15. Какие методы защиты данных можно использовать при работе с системами управления ресурсами предприятия, и как они связаны с управлением жизненным циклом распределенных данных?

#### Критерии оценки:

Раскрытие 90-100% ответа на вопрос - 20 баллов; раскрытие 80-89% ответа на вопрос - 18 баллов; раскрытие 66-79% ответа на вопрос - от 15 баллов; раскрытие 50-65% ответа на вопрос - от 12 баллов; раскрытие менее 50% ответа на вопрос - от 0 до 11 баллов.

## **7.2.2 Комплект отчетов по практическим работам (примеры)**

---

### **7.2.1. Типовые тестовые материалы**

(наименование оценочного средства)

1. **Какое свойство информации означает, что данные доступны только авторизованным пользователям?**

- A) Целостность
- B) Конфиденциальность**
- C) Доступность
- D) Аутентичность

2. **Какой метод защиты от SQL-инъекций является наиболее эффективным?**

- A) Экранирование спецсимволов
- B) Использование параметризованных запросов (prepared statements)**
- C) Ограничение прав доступа к БД
- D) Маскировка ошибок базы данных

3. **Что из перечисленного относится к инструментам статического анализа кода (SAST)?**

- A) OWASP ZAP
- B) Bandit**
- C) SQLMap
- D) Wireshark

4. **Какая уязвимость позволяет злоумышленнику выполнить произвольные команды на сервере через подстановку вредоносного ввода?**

- A) XSS
- B) CSRF
- C) Command Injection**
- D) IDOR

5. **Что такое дифференциальная приватность?**

- A) Метод шифрования данных при передаче
- B) Подход, позволяющий публиковать статистические данные без раскрытия информации о конкретных записях**
- C) Способ защиты от SQL-инъекций
- D) Алгоритм аутентификации пользователей

6. **Какой стандарт описывает требования к системе менеджмента информационной безопасности?**

- A) ISO/IEC 27001**
- B) ISO/IEC 27034
- C) ГОСТ Р 56545-2015
- D) OWASP ASVS

7. **Какая атака на модель машинного обучения заключается в преднамеренном искажении обучающих данных?**

- A) Атака уклонения (evasion attack)
- B) Атака инверсии модели (model inversion)
- C) Отравление данных (data poisoning)**
- D) Атака повторного воспроизведения (replay attack)

8. **Что позволяет реализовать механизм CSRF-защиты в веб-приложениях?**

- A) Проверка реферера запроса
- B) Использование одноразовых токенов в формах**
- C) Ограничение количества запросов с одного IP
- D) Шифрование всех передаваемых данных

9. Какой протокол используется для шифрования передаваемых данных в сети и является основой HTTPS?

- A) SSH
- B) SSL/TLS**
- C) IPsec
- D) SFTP

10. Что такое IDOR (Insecure Direct Object Reference)?

- A) Уязвимость, позволяющая получить несанкционированный доступ к объектам через подстановку идентификатора**
- B) Атака на межсетевой экран
- C) Метод обхода аутентификации
- D) Инструмент для тестирования на проникновение

11. Какой подход позволяет автоматизировать проверки безопасности в процессе разработки и встраивать их в CI/CD?

- A) Agile
- B) DevOps
- C) DevSecOps**
- D) Waterfall

12. Какая уязвимость из OWASP Top 10 связана с неправильной настройкой прав доступа к API, облачным хранилищам и веб-серверам?

- A) SQL Injection
- B) Broken Access Control**
- C) Cross-Site Scripting (XSS)
- D) Security Misconfiguration

13. Что такое гомоморфное шифрование?

- A) Шифрование, позволяющее выполнять вычисления над зашифрованными данными без их расшифровки**
- B) Алгоритм хеширования паролей
- C) Метод защиты от DDoS-атак
- D) Протокол безопасной передачи файлов

14. Какая мера обеспечивает защиту данных при их передаче в облачные хранилища?

- A) Использование VPN
- B) Шифрование на стороне клиента**
- C) Ограничение количества запросов
- D) Мониторинг сетевого трафика

15. Какой инструмент предназначен для динамического тестирования безопасности веб-приложений (DAST)?

- A) OWASP ZAP**
- B) SonarQube
- C) Git
- D) Docker

16. Что из перечисленного относится к методам защиты от атак типа «отказ в обслуживании» (DDoS)?

- A) Использование CDN и фильтрация трафика**
- B) Шифрование данных
- C) Применение параметризованных запросов
- D) Настройка брандмауэра для блокировки ICMP

17. Какое требование безопасности предъявляется к хранению паролей в базе данных?

- A) Хранение в открытом виде
- B) Хранение с использованием необратимого хеширования (с солью)**

С) Шифрование симметричным ключом

Д) Сжатие перед сохранением

18. **Что такое «приватность при обучении с федеративным подходом» (federated learning privacy)?**

А) Модель обучается на централизованном сервере без передачи данных

**В) Данные остаются на устройствах пользователей, передаются только обновления модели**

С) Все данные шифруются перед отправкой на сервер

Д) Применяется дифференциальная приватность к выходным данным модели

19. **Какой этап жизненного цикла данных требует особого внимания с точки зрения безопасности в системах ИИ?**

**А) Сбор и подготовка данных**

В) Обучение модели

С) Инференс

Д) Архивирование

20. **Что из перечисленного является примером безопасной практики при работе с открытым исходным кодом?**

А) Использование любой библиотеки без проверки

**В) Регулярное сканирование зависимостей на наличие известных уязвимостей (SCA)**

С) Копирование кода из интернета без анализа

Д) Игнорирование обновлений безопасности

21. **Какая из перечисленных угроз относится к категории «атаки на веб-приложения» и заключается во внедрении вредоносного кода в веб-страницы?**

**А) XSS (Cross-Site Scripting)**

В) SQL Injection

С) CSRF

Д) Session Hijacking

22. **Что означает принцип наименьших привилегий (least privilege) при управлении доступом?**

А) Пользователи должны иметь максимально возможные права для удобства

**В) Пользователям и процессам предоставляются только те права, которые необходимы для выполнения их функций**

С) Права выдаются на основании иерархии в организации

Д) Все права распределяются по группам безопасности

23. **Какая функция межсетевого экрана (firewall) является основной?**

А) Обнаружение вторжений

**В) Фильтрация сетевого трафика на основе заданных правил**

С) Шифрование данных

Д) Балансировка нагрузки

24. **Что такое двухфакторная аутентификация (2FA)?**

А) Использование двух логинов

**В) Использование двух различных факторов (например, пароль + одноразовый код)**

С) Смена пароля каждые два дня

Д) Использование двух устройств одновременно

25. **Какая уязвимость позволяет злоумышленнику перенаправить запрос пользователя на вредоносный сайт через подмену параметров?**

А) XSS

В) SQL Injection

**С) Open Redirect**

Д) Path Traversal

26. **Что такое сегментирование сети (network segmentation) с точки зрения безопасности?**



**A) Разделение сети на изолированные сегменты для ограничения распространения атак**

B) Подключение всех устройств к одному коммутатору

C) Использование только беспроводных сетей

D) Отключение всех межсетевых экранов

**27. Какой инструмент используется для управления секретами (ключами, паролями) в DevOps-среде?**

A) Jenkins

**B) HashiCorp Vault**

C) Docker

D) Ansible

**28. Что такое «безопасность контейнеров» (container security)?**

A) Использование только официальных образов

**B) Комплекс мер, включающий сканирование образов на уязвимости, ограничение привилегий и изоляцию**

C) Запуск всех контейнеров в привилегированном режиме

D) Использование одной операционной системы для всех контейнеров

**29. Какая из перечисленных атак относится к классу «атаки на модели машинного обучения» и заключается в создании специальных входных данных, заставляющих модель ошибаться?**

A) Атака отравления данных (data poisoning)

**B) Атака уклонения (evasion attack)**

C) Атака инверсии модели (model inversion)

D) Атака подбора выходных данных (membership inference)

**30. Что такое TLS (Transport Layer Security)?**

A) Протокол удалённого доступа

**B) Протокол, обеспечивающий шифрование и целостность данных при передаче по сети**

C) Программа для мониторинга сети

D) Тип межсетевого экрана

**31. Какая мера позволяет обнаружить несанкционированные изменения файлов или данных?**

A) Шифрование

**B) Контроль целостности (хеширование, цифровые подписи)**

C) Сжатие

D) Резервное копирование

**32. Что такое «управление инцидентами безопасности» (incident management)?**

A) Предотвращение всех атак

**B) Процесс обнаружения, анализа, локализации и устранения последствий инцидентов безопасности**

C) Установка обновлений безопасности

D) Обучение сотрудников правилам безопасности

**33. Какая из перечисленных команд позволяет проверить открытые порты на удалённом хосте?**

A) ping

**B) nmap**

C) netstat

D) ifconfig

**34. Что такое «политика безопасности» (security policy) в контексте организации?**

A) Список установленного программного обеспечения

**B) Свод правил, определяющих порядок защиты информации и действий сотрудников**

- C) Описание архитектуры сети
- D) План эвакуации при пожаре

35. **Какая уязвимость из OWASP Top 10 связана с недостаточной защитой сессионных токенов?**

- A) Broken Authentication**
- B) Sensitive Data Exposure
- C) XML External Entities (XXE)
- D) Insecure Deserialization

36. **Что такое «безопасность API» (API security)?**

- A) Защита только баз данных
- B) Комплекс мер, включающий аутентификацию, авторизацию, валидацию входных данных и ограничение частоты запросов для интерфейсов прикладного программирования**
- C) Использование только POST-запросов
- D) Отключение всех API

37. **Какой подход позволяет обеспечить безопасность при использовании сторонних библиотек и компонентов?**

- A) Копирование кода библиотек без изменений
- B) Анализ состава программного обеспечения (SCA) и регулярное обновление зависимостей**
- C) Удаление всех библиотек
- D) Использование только коммерческих компонентов

38. **Что такое «криптографическая защита данных»?**

- A) Сжатие данных для экономии места
- B) Использование алгоритмов шифрования, хеширования и электронной подписи для обеспечения конфиденциальности, целостности и подлинности данных**
- C) Копирование данных на внешние носители
- D) Маскировка данных в логах

39. **Какая мера позволяет обеспечить доступность данных в случае сбоя оборудования или атаки?**

- A) Аутентификация
- B) Резервное копирование и репликация**
- C) Шифрование
- D) Мониторинг

40. **Что такое «безопасность конвейера данных» (data pipeline security) в системах обработки больших данных?**

- A) Использование только одного источника данных
- B) Обеспечение защиты на всех этапах: сбор, передача, хранение, обработка, включая контроль доступа, шифрование и мониторинг**
- C) Хранение всех данных в одной базе
- D) Отключение логирования

### 7.2.2. Типовые примеры заданий

#### Практическая работа №1. Разработка веб-приложения с функцией редактирования заметок и обеспечение базовой безопасности

**Цель работы:** освоить методы безопасной разработки веб-приложений на примере создания функционала редактирования заметок, включая применение безопасных практик кодирования, предотвращение типовых уязвимостей (SQL-инъекции, CSRF, IDOR) и использование современных инструментов анализа безопасности.

**1. Задание:**

Разработать веб-приложение на Python с использованием Flask и SQLAlchemy, реализующее CRUD-операции для управления заметками.

**2. Обеспечить:**

- использование ORM (запрет на конкатенацию SQL-строк);
- защиту от CSRF через Flask-WTF;
- имитацию защиты от IDOR с проверкой прав на основе сессии;
- валидацию и санитизацию ввода;
- наличие минимум двух HTML-шаблонов (главная страница и форма редактирования).

**Форма отчета:**

Исходный код приложения (структура папок, файлы app.py, шаблоны). Скриншоты работающего приложения (главная страница, форма редактирования). Краткий отчёт (1 стр.) с описанием архитектуры, перечнем применённых мер безопасности, пояснением защиты от CSRF и IDOR.

#### Практическая работа №2. Статический анализ кода и устранение уязвимостей

**Цель работы:** научиться использовать инструменты статического анализа кода (SAST) для выявления потенциальных уязвимостей на этапе разработки и устранять найденные проблемы.

**Задание:**

На основе приложения, созданного в ПР №1:

1. Провести статический анализ с помощью Bandit.
2. Проанализировать отчёт, выявить уязвимости (например, hardcoded secrets, debug mode).
3. Устранить уязвимости:
  - вынести секретные данные в переменные окружения (через python-dotenv);
  - отключить режим отладки для production;
  - исправить прочие найденные проблемы.
4. Повторно выполнить анализ и подтвердить устранение.

**Форма отчета:**

Команды запуска Bandit, скриншоты отчётов до и после исправлений.

Фрагменты кода до и после исправлений.

Краткое описание каждой исправленной уязвимости.

## **Практическая работа №3. Динамическое тестирование (DAST) и защита от OWASP Top 10**

**Цель работы:** освоить методы динамического тестирования безопасности веб-приложений, научиться защищать приложение от распространённых уязвимостей (отсутствие заголовков безопасности, CSRF).

### **Задание:**

На основе приложения из ПР №2:

1. Провести активное сканирование с помощью OWASP ZAP.
2. Проанализировать отчёт ZAP, выявить основные уязвимости (например, отсутствие CSP, X-Frame-Options, уязвимость к CSRF).
3. Реализовать защиту:
  - добавить middleware для установки HTTP-заголовков безопасности (CSP, HSTS, X-Frame-Options, X-Content-Type-Options);
  - реализовать полноценную защиту от CSRF (Flask-WTF, если не было в ПР №1);
  - скрыть информацию о сервере (запуск через Gunicorn с кастомным server\_name).
4. Повторно просканировать и подтвердить устранение уязвимостей.

### **Форма отчета:**

1. Скриншоты настройки и запуска сканирования в ZAP.
2. Отчёты ZAP до и после исправлений.
3. Код реализованных защитных механизмов.
4. Краткое описание каждой исправленной уязвимости.

## **Практическая работа №4. Защита от SQL-инъекций и тестирование с помощью SQLMap**

**Цель работы:** углубить понимание механизма SQL-инъекций, научиться защищать приложение с помощью параметризованных запросов и тестировать его устойчивость с помощью специализированных инструментов.

### **Задание:**

Дополнить приложение из ПР №3 функционалом аутентификации (регистрация, логин), используя намеренно уязвимые SQL-запросы с конкатенацией строк (через sqlite3).

1. Провести ручное тестирование SQL-инъекций (обход аутентификации, UNION-атака, time-based) и составить чек-лист.
2. Провести тестирование с помощью SQLMap для уязвимой версии.
3. Переписать уязвимые запросы с использованием параметризованных запросов SQLAlchemy ORM.
4. Повторно протестировать с помощью SQLMap, убедиться в отсутствии уязвимостей.

### **Форма отчета:**

Скриншоты успешных SQL-инъекций (до исправления).

Чек-лист тестирования с payloads.

Команды и результаты SQLMap до и после исправления.

Код уязвимого и безопасного варианта.

Описание принципа работы параметризованных запросов.

## Практическая работа №5. Обеспечение безопасности базы данных PostgreSQL

**Цель работы:** научиться настраивать комплексную безопасность СУБД PostgreSQL на уровне сети, аутентификации, авторизации и шифрования.

**Задание:**

1. Настроить права доступа через pg\_hba.conf: разрешить подключения только с 127.0.0.1 и одного доверенного IP.
2. Реализовать шифрование: сгенерировать SSL-сертификаты через OpenSSL, настроить postgresql.conf для обязательного использования SSL.
3. Создать пользователя приложения с минимальными привилегиями (только SELECT, INSERT), отозвать права у PUBLIC.
4. Настроить брандмауэр ОС для разрешения подключений к порту PostgreSQL только с доверенного IP.

**Форма отчета:**

Фрагменты конфигурационных файлов (pg\_hba.conf, postgresql.conf) с комментариями.

Команды генерации сертификатов и настройки пользователя.

Правила брандмауэра (Windows Firewall / pfctl).

Результаты тестов: успешное подключение с разрешённого IP, блокировка с запрещённого.

## Практическая работа №6. Разработка плана безопасности и DevSecOps-интеграция

**Цель работы:** научиться системно подходить к обеспечению безопасности приложения, разработать комплексный план безопасности и интегрировать проверки в процесс разработки (DevSecOps).

**Задание:**

1. Разработать план безопасности для приложения из ПР №4 с учётом настроек из ПР №5, включающий:
  - цели и требования безопасности;
  - оценку угроз (на основе ранее проведённых тестов);
  - перечень реализованных мер защиты;
  - план регулярного тестирования (SAST, DAST, пентесты).
2. Реализовать CI/CD pipeline (например, через GitHub Actions), который автоматически:
  - запускает Bandit при каждом пуше;
  - блокирует слияние кода при обнаружении критических уязвимостей.

**Форма отчета:**

Документ с планом безопасности (структурированный).

Файл конфигурации CI/CD (например, .github/workflows/security.yml).

Скриншоты из интерфейса CI/CD, показывающие успешный и неуспешный запуски (с блокировкой).

## Практическая работа №7. Мониторинг безопасности и реагирование на инциденты (SIEM Lite)

**Цель работы:** научиться настраивать базовую систему мониторинга безопасности (SIEM-подобную) для сбора, анализа и реагирования на события безопасности веб-приложения и базы данных.

**Задание:**

3. Настроить централизованный сбор логов Flask и PostgreSQL в файлы.
4. Написать Python-скрипт-анализатор, который в реальном времени (или по расписанию) сканирует логи на предмет подозрительных событий.
5. Реализовать автоматическое оповещение (вывод в консоль, запись в файл тревог, отправка email) при обнаружении инцидентов.
6. Сформировать ежедневный отчёт о безопасности (количество запросов, инцидентов, их типы).

**Форма отчета:**

Конфигурации логирования (Flask, PostgreSQL).

Исходный код скрипта-анализатора.

Скриншоты консоли с оповещениями.

Примеры файлов security\_alerts.log и daily\_security\_report.txt.

Краткое описание архитектуры системы мониторинга.

**Общие требования к оформлению отчётов по практическим работам**

Отчёт выполняется в текстовом редакторе, шрифт Times New Roman, 14 pt, межстрочный интервал 1,5, поля – 2 см.

Объём отчёта – не менее 5 страниц (без учёта приложений).

Все графические материалы (схемы, диаграммы, скриншоты) должны быть подписаны и иметь ссылки в тексте.

Код скриптов и конфигурационные файлы могут быть вынесены в приложения.

Отчёт сдаётся преподавателю в электронном виде в установленный срок.

**Критерии оценки за отчеты по практическим работам**

Максимальный балл за каждую работу указан в разделе 4 (таблица содержания дисциплины).

Оценка	Процент от максимума	Критерии
<b>Отлично</b>	85–100%	Задание выполнено полностью, корректно, отчёт содержит цель, ход выполнения, результаты, выводы. При защите студент даёт полные, аргументированные ответы на вопросы.
<b>Хорошо</b>	60–84%	Задание выполнено в полном объёме, но есть незначительные недочёты (неточности в оформлении, неполные выводы, мелкие ошибки). При защите отвечает правильно, но не всегда полно.
<b>Удовлетворительно</b>	30–59%	Задание выполнено частично (не менее 60% требуемого) либо содержит существенные ошибки. При защите затрудняется в ответах.

Оценка	Процент от максимума	Критерии
<b>Неудовлетворительно</b>	0–29%	Работа не выполнена или выполнена менее чем на 60%, отчёт отсутствует, студент не может пояснить ход выполнения.

**Пример:** если работа оценивается в 6 баллов, то «отлично» – 5–6 баллов, «хорошо» – 4 балла, «удовлетворительно» – 2–3 балла, «неудовлетворительно» – 0–1 балл.

### Комплект заданий для итогового теста

#### Задание 1

Какое свойство информации означает, что данные доступны только авторизованным пользователям?

- а) Целостность
- б) Конфиденциальность**
- в) Доступность
- г) Аутентичность

#### Задание 2

Какой метод защиты от SQL-инъекций является наиболее эффективным?

- а) Экранирование спецсимволов
- б) Использование параметризованных запросов (prepared statements)**
- в) Ограничение прав доступа к БД
- г) Маскировка ошибок базы данных

#### Задание 3

Что из перечисленного относится к инструментам статического анализа кода (SAST)?

- а) OWASP ZAP
- б) Bandit**
- в) SQLMap
- г) Wireshark

#### Задание 4

Какая уязвимость позволяет злоумышленнику выполнить произвольные команды на сервере через подстановку вредоносного ввода?

- а) XSS
- б) CSRF
- в) Command Injection**
- г) IDOR

#### Задание 5

Что такое дифференциальная приватность?

- а) Метод шифрования данных при передаче
- б) Подход, позволяющий публиковать статистические данные без раскрытия информации о конкретных записях**
- в) Способ защиты от SQL-инъекций
- г) Алгоритм аутентификации пользователей

### Задание 6

Какой стандарт описывает требования к системе менеджмента информационной безопасности?

- а) ISO/IEC 27001**
- б) ISO/IEC 27034
- в) ГОСТ Р 56545-2015
- г) OWASP ASVS

### Задание 7

Какая атака на модель машинного обучения заключается в преднамеренном искажении обучающих данных?

- а) Атака уклонения (evasion attack)
- б) Атака инверсии модели (model inversion)
- в) Отравление данных (data poisoning)**
- г) Атака повторного воспроизведения (replay attack)

### Задание 8

Что позволяет реализовать механизм CSRF-защиты в веб-приложениях?

- а) Проверка реферера запроса
- б) Использование одноразовых токенов в формах**
- в) Ограничение количества запросов с одного IP
- г) Шифрование всех передаваемых данных

### Задание 9

Какой протокол используется для шифрования передаваемых данных в сети и является основой HTTPS?

- а) SSH
- б) SSL/TLS**
- в) IPsec
- г) SFTP

### Задание 10

Что такое IDOR (Insecure Direct Object Reference)?

- а) Уязвимость, позволяющая получить несанкционированный доступ к объектам через подстановку идентификатора**
- б) Атака на межсетевой экран
- в) Метод обхода аутентификации
- г) Инструмент для тестирования на проникновение

### Задание 11

Какой подход позволяет автоматизировать проверки безопасности в процессе разработки и встраивать их в CI/CD?

- а) Agile
- б) DevOps
- в) DevSecOps**
- г) Waterfall

### Задание 12

Какая уязвимость из OWASP Top 10 связана с неправильной настройкой прав доступа к API, облачным хранилищам и веб-серверам?

- а) SQL Injection
- б) Broken Access Control**



- в) Cross-Site Scripting (XSS)
- г) Security Misconfiguration

### Задание 13

Что такое гомоморфное шифрование?

- а) Шифрование, позволяющее выполнять вычисления над зашифрованными данными без их расшифровки**
- б) Алгоритм хеширования паролей
- в) Метод защиты от DDoS-атак
- г) Протокол безопасной передачи файлов

### Задание 14

Какая мера обеспечивает защиту данных при их передаче в облачные хранилища?

- а) Использование VPN
- б) Шифрование на стороне клиента**
- в) Ограничение количества запросов
- г) Мониторинг сетевого трафика

### Задание 15

Какой инструмент предназначен для динамического тестирования безопасности веб-приложений (DAST)?

- а) OWASP ZAP**
- б) SonarQube
- в) Git
- г) Docker

### Задание 16

Что из перечисленного относится к методам защиты от атак типа «отказ в обслуживании» (DDoS)?

- а) Использование CDN и фильтрация трафика**
- б) Шифрование данных
- в) Применение параметризованных запросов
- г) Настройка брандмауэра для блокировки ICMP

### Задание 17

Какое требование безопасности предъявляется к хранению паролей в базе данных?

- а) Хранение в открытом виде
- б) Хранение с использованием необратимого хеширования (с солью)**
- в) Шифрование симметричным ключом
- г) Сжатие перед сохранением

### Задание 18

Что такое «приватность при обучении с федеративным подходом» (federated learning privacy)?

- а) Модель обучается на централизованном сервере без передачи данных
- б) Данные остаются на устройствах пользователей, передаются только обновления модели**
- в) Все данные шифруются перед отправкой на сервер
- г) Применяется дифференциальная приватность к выходным данным модели

### Задание 19

Какой этап жизненного цикла данных требует особого внимания с точки зрения безопасности в системах ИИ?

- а) Сбор и подготовка данных
- б) Обучение модели
- в) Инференс
- г) Архивирование

#### **Задание 20**

Что из перечисленного является примером безопасной практики при работе с открытым исходным кодом?

- а) Использование любой библиотеки без проверки
- б) Регулярное сканирование зависимостей на наличие известных уязвимостей (SCA)**
- в) Копирование кода из интернета без анализа
- г) Игнорирование обновлений безопасности

#### **Задания открытого типа (дайте развернутый ответ)**

#### **Задание 21**

Дайте определение понятию «DevSecOps». Какие принципы лежат в его основе?

##### **Правильный ответ:**

DevSecOps — подход к разработке программного обеспечения, интегрирующий практики безопасности на всех этапах жизненного цикла (встраивание безопасности в CI/CD, автоматизация проверок безопасности, совместная ответственность команды за безопасность).

#### **Задание 22**

Охарактеризуйте основные типы атак на модели машинного обучения.

##### **Правильный ответ:**

Отравление данных (data poisoning) — внедрение вредоносных данных в обучающую выборку; атака уклонения (evasion attack) — создание специальных входных данных, заставляющих модель ошибаться; атака инверсии модели (model inversion) — восстановление обучающих данных по выходу модели; атака подбора выходных данных (membership inference) — определение, использовалась ли конкретная запись в обучении.

#### **Задание 23**

Что такое дифференциальная приватность и для чего она применяется в системах искусственного интеллекта?

##### **Правильный ответ:**

Дифференциальная приватность — математический подход, гарантирующий, что включение или исключение одной записи из набора данных незначительно влияет на результат вычислений. Применяется для защиты персональных данных при обучении моделей, позволяя публиковать агрегированные результаты без раскрытия информации о конкретных записях.

#### **Задание 24**

Опишите, как организовать защиту конвейера обработки данных (data pipeline) в проекте машинного обучения.

##### **Правильный ответ:**

Защита конвейера включает: контроль доступа к источникам данных, шифрование при передаче и хранении, валидацию и санитизацию входных данных, версионирование и контроль целостности наборов данных, мониторинг аномалий в потоках данных, аудит действий с данными.

### **Задание 25**

Что такое «управление инцидентами информационной безопасности» и каковы основные этапы этого процесса?

#### **Правильный ответ:**

Управление инцидентами — процесс обнаружения, анализа, локализации, устранения и восстановления после нарушений информационной безопасности. Основные этапы: подготовка, идентификация, локализация, искоренение, восстановление, анализ и совершенствование (post-mortem).

### **Задание 26**

Какие меры безопасности необходимо предпринять при развёртывании веб-приложения в облачной среде?

#### **Правильный ответ:**

Настройка правил межсетевого экрана (ограничение доступа), использование безопасных конфигураций (отключение отладочных режимов), регулярное обновление ПО, применение шифрования данных (при передаче и хранении), использование средств управления секретами, внедрение мониторинга и логирования, сканирование на уязвимости перед развёртыванием.

### **Задание 27**

Охарактеризуйте разницу между статическим (SAST) и динамическим (DAST) тестированием безопасности.

#### **Правильный ответ:**

SAST (статический анализ) — анализ исходного кода без его выполнения, выявляет потенциальные уязвимости на ранних этапах разработки. DAST (динамическое тестирование) — анализ работающего приложения, имитирует атаки для обнаружения уязвимостей в среде исполнения. SAST находит проблемы в коде, DAST — в работе системы.

### **Задание 28**

Что такое «безопасность API» и какие методы используются для её обеспечения?

#### **Правильный ответ:**

Безопасность API — комплекс мер, направленных на защиту интерфейсов прикладного программирования от несанкционированного доступа и атак. Методы: аутентификация (JWT, OAuth2), авторизация (контроль доступа), валидация входных данных, ограничение частоты запросов (rate limiting), шифрование трафика (TLS), логирование и мониторинг.

### **Задание 29**

Дайте определение понятию «криптографическая защита данных». Приведите примеры алгоритмов.

#### **Правильный ответ:**

Криптографическая защита — использование математических методов для обеспечения конфиденциальности, целостности и подлинности информации. Примеры алгоритмов: симметричное шифрование (AES), асимметричное шифрование (RSA), хеширование (SHA-256), электронная подпись (ECDSA).

### **Задание 30**

Какие этапы жизненного цикла данных требуют оптимизации с учётом информационной безопасности и почему?

### **Правильный ответ:**

Все этапы: сбор (контроль источников, минимизация данных), передача (шифрование каналов), хранение (шифрование, контроль доступа), обработка (изоляция сред, аудит), архивирование (защита резервных копий), уничтожение (безвозвратное удаление). На каждом этапе необходимо обеспечивать конфиденциальность, целостность и доступность в соответствии с требованиями.

## **7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины**

### **7.3.1 Вопросы к промежуточной аттестации (экзамену)**

1. Что такое обеспечение безопасности при разработке программного обеспечения? Почему это важно?
2. Какие основные угрозы безопасности существуют при разработке ПО?
3. Какие этапы разработки ПО требуют особого внимания к безопасности?
4. Что такое уязвимости в программном обеспечении? Приведите примеры.
5. Какие методы и инструменты используются для выявления уязвимостей в ПО?
6. Что такое DevSecOps? Как этот подход влияет на безопасность ПО?
7. Какие стандарты безопасности существуют для разработки ПО? Приведите примеры.
8. Что такое «безопасный код»? Какие практики помогают писать безопасный код?
9. Как обеспечивается безопасность в процессе непрерывной интеграции и доставки (CI/CD)?
10. Что такое «безопасное программирование»? Какие принципы лежат в его основе?
11. Какие протоколы безопасности используются для защиты данных при передаче по сети?
12. Что такое SSL/TLS? Как они работают?
13. Какие функции выполняют межсетевые экраны в обеспечении безопасности?
14. Какие типы межсетевых экранов существуют? Приведите примеры.
15. Как настраиваются правила межсетевых экранов для защиты сети?
16. Что такое VPN? Как он обеспечивает безопасность передачи данных?
17. Какие инструменты используются для мониторинга сетевого трафика и выявления аномалий?
18. Что такое IDS и IPS? В чем их различия?
19. Как протоколы безопасности и межсетевые экраны взаимодействуют для защиты сети?
20. Какие меры безопасности следует предпринять при настройке удалённого доступа к сети?
21. Какие угрозы безопасности существуют для баз данных?
22. Какие меры безопасности следует предпринять при разработке баз данных?
23. Что такое SQL-инъекция? Как её предотвратить?
24. Какие методы аутентификации и авторизации используются для защиты баз данных?
25. Что такое шифрование данных в базе данных? Какие алгоритмы шифрования используются?
26. Как обеспечивается целостность данных в базе данных?
27. Какие инструменты используются для мониторинга безопасности баз данных?
28. Что такое «безопасная разработка баз данных»? Какие практики это включает?
29. Как обеспечивается резервное копирование и восстановление баз данных?
30. Какие стандарты безопасности существуют для баз данных? Приведите примеры.
31. Что такое сканирование сети? Какие цели оно преследует?
32. Какие инструменты используются для сканирования сети? Приведите примеры.
33. Как проводится сканирование сети на уязвимости?

34. Что такое портовое сканирование? Какие порты считаются уязвимыми?
35. Как сканирование сети помогает выявить потенциальные угрозы?
36. Какие меры безопасности следует предпринять после проведения сканирования сети?
37. Что такое Nmap? Какие функции он выполняет?
38. Как проводится сканирование сети на наличие вредоносного ПО?
39. Какие ограничения существуют при сканировании сети?
40. Как сканирование сети влияет на производительность сети?
41. Какие принципы управления доступом реализуются в СУБД?
42. Какие методы шифрования данных применяются для защиты информации?
43. Какие подходы используются для резервного копирования и восстановления данных?
44. Как осуществляется аудит и мониторинг активности в базах данных?
45. Какие механизмы контроля прав доступа применяются для минимизации рисков?
46. Что такое криптографическая защита данных и как она реализуется?
47. Какие типы атак на веб-приложения наиболее распространены?
48. Как реализуется безопасность в микросервисной архитектуре?
49. Какие методы защиты от XSS-атак применяются в веб-разработке?
50. Как организуется управление инцидентами безопасности в ИТ-системах?
51. Какие принципы безопасности лежат в основе архитектуры приложений?
52. Как обеспечивается безопасность контейнеров в процессе разработки ПО?
53. Какие методы защиты от CSRF-атак применяются в веб-разработке?
54. Как реализуется безопасная аутентификация в распределенных системах?
55. Какие подходы используются для управления секретами в DevOps-практиках?
56. Как обеспечивается безопасность API в современных приложениях?
57. Какие методы защищают от атак типа «человек посередине» (Man-in-the-Middle)?
58. Что такое SAST и DAST? В чем их различия и как они применяются?
59. Какие принципы безопасности следует учитывать при проектировании облачных приложений?
60. Как реализуется безопасная работа с открытым исходным кодом в коммерческих проектах?
61. Какие особенности безопасности возникают при работе с большими данными (распределённое хранение, потоковая обработка)?
62. Что такое дифференциальная приватность и как она применяется для защиты данных в системах машинного обучения?
63. Какие существуют типы атак на модели машинного обучения (отравление данных, атаки с подбором выходных данных, инверсия моделей)? Приведите примеры.
64. Как обеспечить безопасность конвейера данных (data pipeline) при обучении и инференсе моделей?
65. Какие инструменты используются для оценки безопасности моделей машинного обучения (например, Adversarial Robustness Toolbox, TensorFlow Privacy)?
66. Что такое приватность при обучении с федеративным подходом (federated learning) и каковы риски?
67. Как обеспечить безопасное хранение и передачу наборов данных, содержащих персональные данные?
68. Какие методы криптографической защиты данных (гомоморфное шифрование, шифрование с сохранением порядка) актуальны для обработки больших данных?
69. Как организовать мониторинг и аудит доступа к данным в системах ИИ?
70. Какие требования безопасности предъявляются к API, через которые осуществляется взаимодействие с AI-сервисами?
71. Какие этапы жизненного цикла данных требуют оптимизации с учётом безопасности?
72. Какие методы оптимизации управления распределенными данными (сегментирование, репликация, кэширование) влияют на безопасность?

73. Как настроить безопасность в распределённых системах обработки данных (Apache Hadoop, Spark, Kafka)?
74. Какие политики шифрования и управления ключами применяются в распределённых хранилищах данных?

### **Практические кейсы:**

1. Компания подверглась DDoS-атаке через ботнет. Опишите план действий для анализа и устранения атаки. Какие инструменты защиты вы предложите?
2. В облачном хранилище SaaS обнаружена утечка данных из-за ошибки конфигурации. Какие меры нужно срочно принять? Как предотвратить подобное в будущем?
3. Межсетевой экран пропускает трафик с поддельными IP-адресами. В чем может быть причина? Как настроить правила фильтрации правильно?
4. При проведении аудита безопасности выявлена SQL-инъекция в веб-приложении. Разработайте стратегию экстренного реагирования и долгосрочного решения проблемы.
5. В корпоративной сети обнаружены несанкционированные SSH-подключения. Определите источники угрозы и разработайте план защиты.
6. При проведении аудита безопасности выявлено, что модель машинного обучения, развёрнутая в промышленной среде, выдаёт неожиданные результаты при подаче специально сформированных запросов. Опишите возможные причины (атака уклонения) и предложите меры защиты.
7. В проекте используются открытые наборы данных для обучения модели. Как проверить их на наличие вредоносных вкраплений (отравление данных)? Предложите процедуру верификации.
8. Разработайте план обеспечения безопасности для системы, которая собирает данные с IoT-устройств, передаёт их в облако для обучения моделей и предоставляет результаты через веб-сервис. Укажите ключевые точки контроля и меры защиты.
9. Оптимизируйте управление данными в распределённой системе (например, на основе Hadoop) с учётом требований информационной безопасности. Обоснуйте выбор методов и инструментов.

### **Критерии оценивания экзамена при прохождении итогового тестирования по БРС**

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
5	Экзамен (по накопительному рейтингу)	«отлично»	рейтинговый балл 85-100
		«хорошо»	рейтинговый балл 70-84
		«удовлетворительно»	рейтинговый балл 55-69
		«неудовлетворительно»	рейтинговый балл 0-54

## Процедура оценивания по билетам

### 1. Общие положения

Экзамен проводится в устной или письменной форме (по решению преподавателя) с использованием экзаменационных билетов. Каждый билет содержит два теоретических вопроса и один практический кейс. Экзаменуемый должен продемонстрировать знания теоретического материала, понимание основных угроз, методов защиты, а также способность применять полученные знания для анализа и решения практических ситуаций в области обеспечения безопасности при разработке программного обеспечения.

### 2. Требования к ответу

Ответ должен быть научным, логически стройным и опираться на соответствующие теоретические положения, концепции, нормативные документы и научную литературу.

Необходимо строить ответ в единстве теории и практики, подкрепляя теоретические положения примерами из реальной практики разработки программного обеспечения, эксплуатации информационных систем или результатами лабораторных работ.

При ответе на теоретические вопросы следует чётко формулировать определения, классификации, перечислять методы и инструменты, объяснять принципы их работы.

При решении практического кейса требуется:

- определить суть проблемы и возможные причины;
- предложить пошаговый план реагирования;
- обосновать выбор конкретных методов, инструментов или настроек;
- оценить эффективность предлагаемых мер и, при необходимости, предложить долгосрочные решения.

Демонстрация на компьютере не требуется, но экзаменуемый может ссылаться на опыт выполнения лабораторных работ, а также на конкретные команды, конфигурации или инструменты, использованные в ходе практических занятий.

### 3. Порядок ответа

Обучающийся самостоятельно определяет последовательность ответа на вопросы билета.

Время на подготовку – 35 минут. В процессе подготовки разрешается составлять краткий план, выписывать ключевые определения, формулы, схему решения кейса.

После подготовки экзаменуемый последовательно излагает ответы на вопросы билета. Преподаватель может задавать уточняющие и дополнительные вопросы как по содержанию билета, так и по всему курсу.

Оценка объявляется после завершения ответа и обсуждения дополнительных вопросов.

### Критерии оценки:

Оценка	Критерии
«отлично» (85–100 баллов)	Обучающийся полностью раскрыл содержание всех вопросов билета: даны исчерпывающие, аргументированные ответы, демонстрирующие глубокое понимание материала. Практический кейс решён верно, предложены обоснованные меры реагирования и защиты, использованы профессиональные термины. Ответ логичен, грамотен,

Оценка	Критерии
	структурирован. На дополнительные вопросы даны правильные ответы.
«хорошо» (70–84 балла)	Обучающийся полно раскрыл содержание вопросов билета, но допустил незначительные неточности или ошибки в деталях, не влияющие на общее понимание. Практический кейс решён в целом верно, но возможны несущественные замечания по полноте или обоснованию. На дополнительные вопросы ответил правильно или с небольшими уточнениями.
«удовлетворительно» (55–69 баллов)	Обучающийся раскрыл основные вопросы билета, но допустил существенные ошибки в деталях, либо ответы носят поверхностный характер. Практический кейс решён не полностью, отсутствует часть предложенных мер или их обоснование. Затрудняется при ответе на дополнительные вопросы.
«неудовлетворительно» (0–54 балла)	Обучающийся не раскрыл содержание вопросов билета, допустил принципиальные ошибки, не решил практический кейс или предложил неверные решения. Не может ответить на дополнительные вопросы.



## 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1 Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Баранова Е. К.	Криптографические методы защиты информации : лаб. практикум : учеб. пособие / Е. К. Баранова, А. В. Бабаш. - Москва : Кнорус, 2015. - 196 с. : ил. + CD. - (Бакалавриат). - Библиогр. в конце гл. - ISBN 978-5-406-03802-4 : 250-00. - ISBN 205-00.	Учебное пособие	2015	2
2	Фороузан Б. А.	Криптография и безопасность сетей [Электронный ресурс] : учеб. пособие / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина . - Москва : ИНТУИТ, 2017 ; Саратов : Вузовское образование, 2017. - 782 с. : ил. - (Основы информационных технологий). - ISBN 978-5-4487-0143-6.	Учебное пособие	2017	ЭБС «IPRbooks»
3	Хорев П. Б.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие / П. Б. Хорев. - 2-е изд., испр. и доп. - Москва : Форум : ИНФРА-М, 2015. - 352 с. - (Высшее образование). - ISBN 978-5-00091-004-7.	Учебное пособие	2015	ЭБС «Znanium.com»

### 8.3 Дополнительная литература

№ п/п	Авторы, со- ставители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методиче- ское пособие, практикум, др.)	Год из- дания	Количество в научной биб- лиотеке / Наименова- ние ЭБС
1	Кукина Е. Г.	Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. - Омск : ОмГУ, 2013. - 91 с. - ISBN 978-5-7779-1588-7.	Учебное пособие	2013	ЭБС «IPRbooks»
2	Никифоров С. Н.	Защита информации [Электронный ресурс] : учеб. пособие / С. Н. Никифоров. - Санкт-Петербург : СПбГАСУ, 2015. - 383 с. : ил. - ISBN 978-5-9227-0585-1.	Учебное пособие	2015	ЭБС «IPRbooks»
3	Спицын В. Г.	Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын. - Томск : Эль Контент, 2011. - 148 с. - ISBN 978-5-4332-0020-3.	Учебное пособие	2011	ЭБС «IPRbooks»
4	Федин Ф. О.	Информационная безопасность [Электронный ресурс] : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин ; [под ред. В. А. Дикарева]. - Москва : МГПУ, 2011. - 260 с.	Учебное пособие	2011	ЭБС «IPRbooks»

### 8.3 Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	Springer Nature (Полнотекстовая коллекция журналов)	<a href="https://www.springernature.com/gp/products">https://www.springernature.com/gp/products</a>
2	Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature)	<a href="https://link.springer.com/">https://link.springer.com/</a>
3	«Кодекс»	<a href="https://kodeks.ru/">https://kodeks.ru/</a>
4	Техэксперт	<a href="https://cntd.ru/">https://cntd.ru/</a>
5	Федеральная служба по техническому и экспортному контролю	<a href="http://fstec.ru/">http://fstec.ru/</a>
6	Kaggle (датасеты с метками безопасности)	<a href="#">Kaggle датасеты: полное руководство по поиску и использованию для анализа данных - DataLopata</a>

### 8.4 Перечень программного обеспечения

№ п/п	Наименование ПО	Количество лицензий	Реквизиты договора (дата, номер, срок действия)
1	Visual Studio Code (VS Code)	неограниченный	Бесплатное ПО, лицензия MIT
2	Eclipse IDE	неограниченный	Бесплатное ПО, лицензия Eclipse Public License (EPL)
3	JUnit	неограниченный	Бесплатное ПО, лицензия Eclipse Public License (EPL)
4	SonarQube	неограниченный	Бесплатное ПО, лицензия GNU LGPL
5	Git	неограниченный	Бесплатное ПО, лицензия GPLv2
6	GitHub	неограниченный	Бесплатное ПО, лицензия MIT
7	OWASP ZAP (Zed Attack Proxy)	неограниченный	Бесплатное ПО, лицензия Apache License 2.0
8	Wireshark	неограниченный	Бесплатное ПО, лицензия GPLv2

- Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий	Перечень основного оборудования
-------	---	---------------------------------

1	Компьютерный класс. Помещение для самостоятельной работы. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (Г-401)	Столы ученические, стулья ученические, ПК с выходом в сеть Интернет
2	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-408)	Компьютер (монитор 17", системный блок Intel (R) Celeron (R) 2,66 GHz / 1 Gb / 80 Gb), маршрутизатор 2801 Router, коммутатор Catalyst, экран/интерактивная доска Smart Board TB, проектор Acer P1303W., стол преподавательский, стол ученический, стол компьютерный, стул, доска аудиторная (маркерная).
3	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-418)	Стол ученический двухместный (моноблок), доска аудиторная 3-х секционная (меловая), стол преподавательский, стул, проектор Acer