

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

Б1.О.20

(индекс дисциплины)

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Обеспечение безопасности при разработке программного обеспечения**

(наименование дисциплины)

по направлению подготовки  
09.03.04 Программная инженерия

направленность (профиль)  
Программная инженерия с применением ИИ-технологий

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 5 ЗЕ

**Распределение часов дисциплины по семестрам**

Семестр	7	Итого
Вид занятий	экзамен	
Лекции	16	16
Лабораторные		
Практические	32	32
Руководство: курсовые работы (проекты) / РГР		
Промежуточная аттестация	0,35	0,35
Контактная работа	48,35	48,35
Самостоятельная работа	96	96
Контроль	35,65	35,65
<b>Итого</b>	<b>180</b>	<b>180</b>

Рабочую программу составил:

доцент института цифровых технологий, канд. экон. 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

09.03.04 Программная инженерия

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

---

**Срок действия рабочей программы дисциплины до «31» августа 2030 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 с применением технологий искусственного интеллекта, включая методы защиты данных, моделей и процессов разработки.

### Задачи:

1. Изучение типовых уязвимостей программного обеспечения и методов их предотвращения, с акцентом на уязвимости в системах, использующих ИИ.
2. Знакомство с принципами проектирования безопасного программного обеспечения, включая защиту данных на всех этапах жизненного цикла разработки.
3. Изучение методов и средств аутентификации и авторизации пользователей в распределённых системах обработки данных.
4. Знакомство с криптографическими методами и средствами защиты данных, включая современные подходы (гомоморфное шифрование, дифференциальная 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 (TensorFlow Privacy, Adversarial Robustness Toolbox и др.).
8. Формирование умения анализировать уязвимости программного обеспечения и разрабатывать политику информационной безопасности для проектов в области программной инженерии с применением ИИ.
9. Овладение приёмами 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 в структуре ОПОП ВО

Дисциплина относится к **обязательной части** блока Б1.

Дисциплины, на освоении которых базируется данная дисциплина:

Информационные системы и технологии, Управление проектами разработки программного обеспечения, Базы данных и управление данными, Обеспечение качества кода и код ревью.

Дисциплины, для которых необходимы знания, умения, навыки, приобретаемые в результате изучения данной дисциплины:

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: источники профессиональной информации; основы библиографического описания; основные угрозы информационной безопасности и методы защиты. Уметь: формулировать поисковые запросы; соблюдать правила цитирования. Владеть: навыками безопасной работы в сети
	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.	Знать: типовые задачи (поиск аналогов, анализ существующих решений). Уметь: использовать ИКТ для сбора и обработки информации; применять базовые меры защиты информации (шифрование, аутентификация). Владеть: навыками написания литературных обзоров с соблюдением авторских прав.
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Знать: стандарты оформления научных работ (ГОСТы). Уметь: структурировать и представлять результаты исследования. Владеть: навыками работы с системами антиплагиата и правильного оформления заимствований.
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: системные требования, зависимости, порядок установки ОС, драйверов, прикладного ПО. Уметь: планировать процесс установки. Владеть: навыками поиска и разрешения конфликтов совместимости.
	ОПК-5.2. Умеет выполнять настройку информационных и автоматизированных систем	Знать: основные параметры конфигурации ОС, сетевых служб, СУБД. Уметь: производить тонкую настройку систем для достижения требуемой производительности и безопасности. Владеть: навыками работы с системным реестром, конфигурационными файлами.
	ОПК-5.3. Владеет навыками установки программного и аппаратного обеспечения	Знать: методы автоматизированной установки (скрипты, образы). Уметь: выполнять полный цикл развертывания системы "с нуля".

<b>Формируемые и контролируемые компетенции</b> (код и наименование)	<b>Индикаторы достижения компетенций</b> (код и наименование)	<b>Планируемые результаты обучения</b>
	информационных и автоматизированных систем	Владеть: практическими навыками установки и настройки всего необходимого ПО для работы стека разработки.

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

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
1. Основы безопасности ПО и управления данными	лекция	Тема 1. Введение в безопасность при разработке программного обеспечения. Особенности безопасности систем с применением ИИ.	7	2	—	—	—
	самост.	Изучение лекционного материала, подготовка к практическим занятиям	7	10	—	—	—
	лекция	Тема 1.1. Методы оптимизации управления жизненным циклом распределённых данных с учётом информационной безопасности. Приватность данных и дифференциальная приватность.	7	2	—	—	—
	самост.	Изучение лекционного материала, подготовка к практическим занятиям	7	20	—	—	—
2. Безопасность в сетевых технологиях и системах ИИ	лекция	Тема 2. Принципы информационной безопасности. Проектирование безопасности для систем сбора и обработки больших данных.	7	2	—	—	—
	практ.	Практическая работа №1. Разработка веб-приложения с функцией редактирования заметок и обеспечение базовой безопасности (Flask, защита от CSRF, IDOR).	7	4	15	—	Отчёт по практической работе (защита)

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
	практ.	Практическая работа №2. Статический анализ кода и устранение уязвимостей. Применение к коду, работающему с данными для обучения моделей.	7	4	10	–	Отчёт по практической работе (защита)
	практ.	Практическая работа №3. Динамическое тестирование (DAST) и защита от OWASP Top 10. Проверка уязвимостей в приложениях, загружающих данные из внешних источников.	7	4	15	–	Отчёт по практической работе (защита)
	практ.	Практическая работа №4. Защита от SQL-инъекций и тестирование с помощью SQLMap. Применение к базам данных, используемым для хранения признаков наборов.	7	4	15	–	Отчёт по практической работе (защита)
	практ.	Практическая работа №5. Обеспечение безопасности базы данных PostgreSQL. Настройка прав доступа и шифрования для хранилища данных, содержащего персональные данные.	7	6	15	–	Отчёт по практической работе (защита)
	практ.	Практическая работа №6. Разработка плана безопасности и DevSecOps-интеграция. Включение проверок безопасности данных и моделей в CI/CD.	7	6	15	–	Отчёт по практической работе (защита)

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы	Интер-актив, ч	Формы текущего контроля
	практ.	Практическая работа №7. Мониторинг безопасности и реагирование на инциденты (SIEM Lite). Отслеживание аномалий в доступе к данным и работе моделей.	7	4	15	–	Отчёт по практической работе (защита)
	самост.	Изучение лекционного материала, подготовка к практическим занятиям	7	16	–	–	–
	лекция	Тема 3. Технология осуществления оптимизации управления жизненным циклом данных. Безопасность конвейеров обработки данных.	7	2	–	–	–
	самост.	Изучение лекционного материала	7	4	–	–	–
	лекция	Тема 4. Инструменты, используемые для обеспечения безопасности на этапе разработки. Инструменты для анализа безопасности данных и моделей (TensorFlow Privacy, Adversarial Robustness Toolbox и др.).	7	2	–	–	–
	самост.	Изучение лекционного материала	7	10	–	–	–
3. Разработка прикладных задач с учётом требований безопасности (в т.ч. для ИИ)	лекция	Тема 5. Оптимизация управления жизненным циклом данных. Обеспечение безопасности при использовании внешних наборов данных и моделей.	7	2	–	–	–



Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы	Интерактив, ч	Формы текущего контроля
	самост.	Изучение лекционного материала	7	10	–	–	–
	лекция	Тема 6. Угрозы безопасности и методы их предотвращения. Атаки на модели машинного обучения (отравление данных, инверсия, уклонение).	7	2	–	–	–
	самост.	Изучение лекционного материала	7	10	–	–	–
	лекция	Тема 7. Реагирование на угрозы безопасности. Создание систем мониторинга и защиты для AI-сервисов.	7	2	–	–	–
	самост.	Изучение лекционного материала	7	16	–	–	–
	пром. аттест.	Промежуточная аттестация	7	0,35	–	–	–
	контроль	Экзамен	7	35,65	100	–	Итоговый тест
<b>Итого</b>				<b>180</b>	<b>100</b>	–	

**Схема расчета итогового балла:**

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

## **5. Образовательные технологии**

В рамках изучения дисциплины предусмотрено использование следующих образовательных технологий:

- технология традиционного обучения;
- интерактивные технологии: учебные дискуссии (применяются во всех модулях по итогам выполнения работ).

Технологии традиционного обучения - организация учебного процесса в вузе, основанная на лекционных и практических формах обучения: объяснительно-иллюстративное обучение. Данная технология применяется во всех модулях курса.

Технология интерактивного обучения — это организация учебного процесса, которая предполагает максимальную активность обучающихся в процессе формирования ключевых компетенций. На учебной дискуссии обучающиеся представляют результаты выполнения заданной работы. Проводится обсуждение применённых решений, их эффективности и архитектуры программного кода.

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

### **6.1 Рекомендации по подготовке к практическим занятиям**

Обучающимся следует:

- при подготовке к занятиям обязательно использовать не только учебную литературу, но и другие источники;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание путей решения поставленных задач и освоения выданных знаний, в случае затруднений обращаться к преподавателю.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если обучающийся видит несколько путей решения задачи, то нужно сравнить их и выбрать самый рациональный. Полезно до начала решения задачи составить краткий план решения задачи. Решение проблемных задач или примеров следует излагать подробно, отделяя вспомогательные пути решения от основных. Решения при необходимости нужно сопровождать комментариями, схемами, алгоритмами.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

### **6.2 Рекомендации по подготовке к итоговой сдаче дисциплины**

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

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

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
7	ОПК-3; ОПК-5	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)

### 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 отчет (1 стр.) с описанием архитектуры, перечнем применённых мер безопасности, пояснением защиты от CSRF и IDOR.

Критерии оценки:

Показатель	Макс. балл
Полнота реализации CRUD-функционала	5
Корректное использование ORM (безопасные запросы)	4
Реализация CSRF-защиты (Flask-WTF)	3
Реализация имитации защиты от IDOR	2
Качество отчёта и оформление	1
Итого	15

#### 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.

Критерии оценки:

Показатель	Макс. балл
Корректное выполнение статического анализа (Bandit)	2
Полнота выявления уязвимостей	2
Качество исправлений (вынос секретов, отключение debug)	3
Подтверждение устранения (скриншоты повторного сканирования)	2
Оформление отчёта	1
Итого	10

**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.

**Критерии оценки:**

Показатель	Макс. балл
Корректное выполнение DAST (ZAP)	4
Полнота выявления уязвимостей	4
Качество реализации защитных заголовков и CSRF	3
Подтверждение устранения (скриншоты повторного сканирования)	3
Оформление отчёта	1
Итого	15

**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.

Критерии оценки:

Показатель	Макс. балл
Корректная реализация уязвимой и защищённой версий	4
Полнота ручного тестирования (чек-лист)	4
Корректное использование SQLMap	3
Демонстрация устранения уязвимостей	2
Оформление отчёта	1
Итого	15

### 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.

Критерии оценки:

Показатель	Макс. балл
Корректность настройки pg_hba.conf	4
Корректность настройки SSL	4
Корректность настройки прав пользователя и отзыва прав у PUBLIC	3
Настройка брандмауэра и подтверждение работы	2
Оформление отчёта	1

Показатель	Макс. балл
Итого	15

### 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:

- 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).
- 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).

#### Критерии оценки:

Показатель	Макс. балл
Полнота и структурированность плана безопасности	4
Корректность описания угроз и мер защиты	4
Реализация CI/CD pipeline (автоматизация SAST)	3
Демонстрация работы pipeline (блокировка плохого кода)	2
Оформление отчёта	1
Итого	15

## 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.

Критерии оценки:

Показатель	Макс. балл
Корректность настройки сбора логов	4
Функциональность скрипта-анализатора (обнаружение 3+ типов инцидентов)	4
Реализация автоматического оповещения и отчётов	3
Полнота документации и скриншотов	2
Оформление отчёта	1
Итого	15

### 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.

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

#### **7.3.1 тестации (экзамену)**

#### **Вопросы к промежуточной аттестации**

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 распределёнными 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:**

Кейс 1. В веб-приложении обнаружена SQL-инъекция. Разработайте план немедленного реагирования и долгосрочного устранения уязвимости. Какие инструменты используете для проверки?

Кейс 2. При динамическом тестировании OWASP ZAP выявлено отсутствие HTTP-заголовков безопасности (CSP, HSTS, X-Frame-Options). Какие заголовки необходимо добавить и как это повлияет на безопасность приложения?

Кейс 3. Модель машинного обучения, развёрнутая в промышленной среде, стала выдавать неожиданные результаты при подаче специально сформированных запросов. Предположите причину (атака уклонения) и предложите меры защиты.

Кейс 4. Разрабатывается система, которая собирает данные с IoT-устройств, передаёт их в облако для обучения моделей и предоставляет результаты через веб-сервис. Укажите ключевые точки контроля безопасности и предложите меры защиты на каждом этапе.

Кейс 5. В CI/CD pipeline (GitHub Actions) необходимо интегрировать проверки безопасности: статический анализ кода, сканирование зависимостей, проверку секретов. Опишите, как это можно реализовать, и какие инструменты использовать.

Кейс 6. Проект использует открытые наборы данных для обучения модели. Как проверить их на наличие вредоносных вкраплений (отравление данных)? Предложите процедуру верификации.

Кейс 7. В корпоративной сети обнаружены несанкционированные SSH-подключения к серверу с обучающими данными. Определите возможные источники угрозы и разработайте план защиты.

Кейс 8. Для облачного хранилища, содержащего персональные данные, требуется настроить шифрование и управление ключами. Какие механизмы вы предложите (шифрование на стороне клиента, управление ключами в KMS, ротация ключей)?

Кейс 9. При развёртывании модели через API были зафиксированы аномально высокие запросы от одного IP-адреса. Какие меры необходимо принять для предотвращения атаки перебора (brute-force) или DoS?

Кейс 10. Разработайте план обеспечения безопасности для системы, использующей федеративное обучение на мобильных устройствах. Укажите меры защиты на стороне клиента и сервера.

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

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
7	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,



Оценка	Критерии
	грамотен, 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, составители	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 самостоятель-	Столы ученические, сту-

	ной 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)	для 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 TV, 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