МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Безопасность программного обеспечения

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Безопасность программного обеспечения", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-13 - Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

ОПК-15 - Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем;

ОПК-7.3. - Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Проводит комплексный поиск и классификацию уязвимостей в ПО с использованием автоматизированных средств и методологий атак.

Настраивает и контролирует работу средств защиты ПО на стадиях развертывания и эксплуатации, анализирует события безопасности.

Проводит верификацию кода на соответствие стандартам безопасной разработки и требованиям нормативных документов.

Результаты обучения по дисциплине:

Знать классификацию уязвимостей по системам CWE и CVE, основные векторы атак из списка OWASP Top 10, принципы работы инструментов DAST и фаззинг-тестирования.

Знать механизмы защиты контейнеризированных приложений (Docker, K8s) и управления секретами. Принципы мониторинга прикладного уровня и роль SIEM-систем в анализе логов. Протоколы безопасной аутентификации и авторизации (OAuth 2.0, JWT).

Знать требования стандартов безопасной разработки (ГОСТ Р 56939, ISO/IEC 27034). Методологии моделирования угроз (STRIDE, DREAD). Технологии SAST (статический анализ) и методы противодействия реверс-инжинирингу (обфускация).

Уметь выявлять логические и инъекционные уязвимости (SQLi, XSS) в работающих приложениях; Проводить фаззинг-тестирование функций обработки входных данных для поиска ошибок исполнения.

Уметь администрировать средства разграничения доступа в Web-приложениях и API. Настраивать логирование критических событий безопасности в ПО для последующего аудита.

Уметь разрабатывать модель угроз для конкретного программного модуля или информационной системы. Использовать статические анализаторы кода для поиска «опасных» функций и дефектов безопасности.

Владеть навыками эксплуатации типовых уязвимостей (переполнение буфера, Path Traversal) в учебных целях для проверки эффективности защиты.

Владеть инструментами мониторинга защищенности инфраструктуры развертывания (сканеры образов, анализаторы конфигураций).

Владеть методами верификации криптографических механизмов (проверка алгоритмов хеширования и хранения ключей). Навыками внедрения практик DevSecOps в жизненный цикл разработки ПО.

2 Место дисциплины "Безопасность программного обеспечения" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность операционных систем, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Нормативные требования по защите информации, Информационные угрозы.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Безопасность программного обеспечения" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Безопасность программного обеспечения" составляет 4 зачетных единицы, 144 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 3/Семестр 5			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия			
Практические занятия	32		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	26		
Самостоятельная работа	18		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Безопасность программного обеспечения", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
Раздел 1. Введение и основы безопасности ПО	
Тема 1. Введение в безопасность ПО. Основные понятия (конфиденциальность, целостность, доступность), аксиоматика безопасности, классификация угроз и нарушителей.	2
Тема 2. Законодательная и нормативная база. Правовые аспекты ИБ (УК РФ, ФЗ-152), стандарты безопасной разработки (ГОСТ Р 56939, ISO/IEC 27034).	2
Тема 3. Моделирование угроз. Методологии STRIDE, DREAD, построение деревьев атак и профилирование нарушителя.	4
Раздел 2. Уязвимости и атаки	
Тема 4. Классификация уязвимостей ПО. Системы CWE и CVE. Основные риски по версии OWASP Top 10.	2
Тема 5. Уязвимости управления памятью. Переполнение буфера (стек, куча), форматные строки, ошибки работы с указателями.	2

Тема 6. Логические и инъекционные уязвимости. SQL-инъекции, Cross-Site Scripting (XSS), Path Traversal, небезопасная десериализация.	2
Раздел 3. Безопасная разработка (S-SDLC)	
Тема 7. Жизненный цикл безопасной разработки (S-SDLC). Интеграция безопасности в Agile/DevOps. Концепция DevSecOps.	2
Тема 8. Методы статического анализа (SAST). Принципы работы анализаторов исходного кода, поиск подозрительных конструкций.	2
Тема 9. Динамический анализ и фаззинг-тестирование (DAST/Fuzzing). Генерация случайных входных данных для поиска ошибок исполнения.	2
Раздел 4. Специализированные аспекты и защита	
Тема 10. Криптографические методы в ПО. Безопасное хранение паролей, использование хеш-функций и симметричного/асимметричного шифрования.	2
Тема 11. Безопасность Web-приложений и API. Протоколы OAuth 2.0, JWT, защита микросервисной архитектуры.	2
Тема 12. Реверс-инжиниринг и обфускация. Методы защиты кода от анализа (анти-отладка, упаковщики) и способы их обхода.	2
Раздел 5. Администрирование и аудит	
Тема 13. Безопасность развертывания и инфраструктуры. Контейнеризация (Docker, K8s), управление секретами.	2
Тема 14. Мониторинг, логирование и реагирование. Роль систем SIEM в обнаружении атак на прикладном уровне.	4
Итого	**32**

4.2. Практические занятия

Наименование работы	**Трудоемкость в часах**
	ОФ
1. Основы, нормы и проектирование (Темы 1–3) 1. **Кейс-стади «Триада КИД»**: Для трех разных систем (онлайн-банк, АСУ ТП завода, вики-ресурс) расставить приоритеты между Конфиденциальностью, Целостностью и Доступностью. Обосновать выбор. 2. **Аудит соответствия**: Изучить требования **ГОСТ Р 56939** и составить чек-лист для проверки гипотетического IT-стартапа на готовность к сертификации. 3. **Моделирование STRIDE**: Используя инструмент **OWASP Threat Dragon** или Microsoft Threat Modeling Tool, построить DFD-диаграмму для модуля авторизации и выявить минимум 5 угроз.	6

2. **Анализ уязвимостей и атак (Темы 4–6)** 1. **Работа с базами CVE/CWE**: Найти в реестре CVE уязвимость в популярном ПО (например, Chrome или WordPress) за последний год и сопоставить её с классификатором CWE. 2. **Лабораторная «Buffer Overflow»**: В безопасной среде (например, на платформе **TryHackMe** или локально с отключенной защитой ASLR) провести атаку переполнения стека, чтобы изменить значение переменной или вызвать Shell. 3. **Взлом и защита (Web)**: На стенде **OWASP Juice Shop** или **DVWA** реализовать три атаки: SQL-инъекцию (обход логина), XSS (кража cookie) и Path Traversal.	6
3. Процессы и инструменты (Темы 7–9) 1. **Проектирование DevSecOps-пайплайна**: Нарисовать схему CI/CD, указав, на каких этапах внедряются инструменты SAST, DAST и проверка зависимостей (SCA). 2. **Статический анализ кода (SAST)**: Прогнать проект на GitHub через бесплатный сканер (например, **SonarQube** или **Snyk**) и составить отчет по найденным «security smells». 3. **Фаззинг-тестирование**: Написать простой фаззер на Python для тестирования сетевого сервиса или функции обработки строк на предмет аварийного завершения (Crash).	8
4. Криптография и Web (Темы 10–11) 1. **Безопасное хранилище**: Реализовать на языке программирования (Python/Java/C#) функцию регистрации пользователя с использованием **Salted Hashing** (библиотека bcrypt) и объяснить, почему нельзя использовать MD5. 2. **JWT Debugging**: Используя сервис jwt.io, «разобрать» токен, изменить его полезную нагрузку и попытаться понять, как сервер обнаружит подделку (проверка сигнатуры).	4
5. Инфраструктура и мониторинг (Темы 12–14) 1. **Reverse Engineering**: С помощью утилиты **Ghidra** или **IDA Free** проанализировать простой CrackMe-бинарник и найти в нем зашитый пароль или логику проверки ключа. 2. **Hardening Docker**: Проверить Docker-образ на уязвимости (утилита **Trivy**) и переписать Dockerfile, чтобы избавиться от запуска под пользователем root. 3. **Анализ логов**: В предоставленном текстовом файле логов веб-сервера (Apache/Nginx) вручную или скриптом найти следы сканирования портов и попыток SQL-инъекции.	8
Итого	**32**

4.3 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Наименование работы Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	6
Оформление отчетов по практическим и(или) лабораторным работам	6
Подготовка к промежуточной аттестации	6
Итого	**18**

Самостоятельная работа под руководством преподавателя	26
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Безопасность программного обеспечения"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-13	Проводит комплексный поиск и классификацию уязвимостей в ПО с использованием автоматизированных средств и методологий атак.	**Знать** классификацию уязвимостей по системам **CWE** и **CVE**, основные векторы атак из списка **OWASP Top 10**, принципы работы инструментов **DAST** и фаззинг-тестирования. **Уметь** выявлять логические и инъекционные уязвимости (SQLi, XSS) в работающих приложениях; Проводить фаззинг-тестирование функций обработки входных данных для поиска ошибок исполнения. **Владеть** навыками эксплуатации типовых уязвимостей (переполнение буфера, Path Traversal) в учебных целях для проверки эффективности защиты.	Высокий или средний

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-15	Настраивает и контролирует работу средств защиты ПО на стадиях развертывания и эксплуатации, анализирует события безопасности.	**Знать** механизмы защиты контейнеризированных приложений (**Docker, K8s**) и управления секретами. Принципы мониторинга прикладного уровня и роль **SIEM-систем** в анализе логов. Протоколы безопасной аутентификации и авторизации (OAuth 2.0, JWT). **Уметь** администрировать средства разграничения доступа в Web-приложениях и API. Настраивать логирование критических событий безопасности в ПО для последующего аудита. **Владеть** инструментами мониторинга защищенности инфраструктуры развертывания (сканеры образов, анализаторы конфигураций).	
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-7.3	Проводит верификацию кода на соответствие стандартам безопасной разработки и требованиям нормативных документов.	**Знать** требования стандартов безопасной разработки (**ГОСТ Р 56939**, ISO/IEC 27034). Методологии моделирования угроз (**STRIDE**, DREAD). Технологии **SAST** (статический анализ) и методы противодействия реверс-инжинирингу (обфускация). **Уметь** разрабатывать модель угроз для конкретного программного модуля или информационной системы. Использовать статические анализаторы кода для поиска «опасных» функций и дефектов безопасности. **Владеть** методами верификации криптографических механизмов (проверка алгоритмов хеширования и хранения ключей). Навыками внедрения практик **DevSecOps** в жизненный цикл разработки ПО.	Высокий или средний

Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено.
Средний уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено.
Низкий уровень достижения компетенции - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

тестирование по разделу дисциплины

Обучающийся отвечает на 10 тестовых заданий.

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень тестовых заданий:

Компетенция ОПК-13: Диагностика, тестирование и анализ уязвимостей

1. **При использовании методологии DREAD, какой параметр отвечает за оценку того, насколько легко злоумышленнику будет использовать уязвимость?**

A) Damage (Ущерб)
B) Reproducibility (Воспроизводимость)
C) **Exploitability (Исчерпаемость/Простота использования)**
D) Discoverability (Обнаруживаемость)

1. **Для выявления уязвимости «Path Traversal» наиболее эффективным методом динамического тестирования является:**

A) Статический анализ исходного кода
B) **Фаззинг-тестирование с подстановкой последовательностей ../ в параметры запроса**
C) Проверка контрольных сумм исполняемых файлов
D) Анализ прав доступа в Active Directory

1. **В системе классификации уязвимостей, что означает идентификатор CVE?**

A) Описание общих типов программных ошибок (Common Weakness Enumeration)
B) **Уникальный номер конкретной уязвимости в конкретном ПО (Common Vulnerabilities and Exposures)**
C) Метрика критичности уязвимости от 0 до 10
D) Протокол передачи данных о взломе

Компетенция ОПК-15: Администрирование, контроль и мониторинг

1. **Какая технология позволяет безопасно передавать секреты (пароли, API-ключи) в контейнеризированные приложения Docker/K8s (Тема 13)?**

A) Прописывание паролей в переменные окружения в Dockerfile
B) **Использование специализированных хранилищ (HashiCorp Vault, Kubernetes Secrets)**
C) Хранение паролей в открытом виде в Git-репозитории
D) Передача секретов через незашифрованные HTTP-заголовки

1. **Основная задача SIEM-системы при мониторинге безопасности ПО — это:**

A) Автоматическое исправление ошибок в коде
B) **Сбор, корреляция событий из разных источников и выявление аномалий в реальном времени**
C) Резервное копирование баз данных
D) Шифрование жестких дисков серверов

1. **При администрировании API, какой механизм обеспечивает безопасную передачу прав доступа между сервисами без передачи пароля пользователя (Тема 11)?**

A) Базовая аутентификация (Login/Pass)
B) **Протокол OAuth 2.0 / JWT-токены**
C) Симметричное шифрование DES
D) Хранение сессий в Cookies без флага HttpOnly

Компетенция ОПК-7.3: Анализ защищенности и верификация ПО

1. **Какая функция в языке C++ считается небезопасной и может привести к переполнению буфера (Тема 5)?**

A) strncpy()
B) **gets()**

1. C) printf("%s", str)

D) std::vector::at()

1. **В чем заключается основное отличие статического анализа (SAST) от динамического (DAST)?**

A) SAST требует запуска программы, DAST — нет
B) **SAST анализирует исходный код или байт-код без запуска, DAST тестирует работающее приложение**
C) SAST ищет только ошибки в логике, DAST — только ошибки в синтаксисе
D) Между ними нет разницы

1. **При верификации криптографической защиты паролей, какой подход является наиболее надежным ?**

A) Шифрование алгоритмом AES-256 с хранением ключа в коде
B) Хеширование алгоритмом MD5
C) **Использование адаптивных функций хеширования (Argon2, bcrypt) с солью (salt)**
D) Хранение паролей в Base64

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 20 тестовых заданий

Критерии оценивания при тестировании:
- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень тестовых заданий:

Компетенция ОПК-13: Диагностика, тестирование и анализ уязвимостей

1. **При использовании методологии DREAD, какой параметр отвечает за оценку того, насколько легко злоумышленнику будет использовать уязвимость?**

A) Damage (Ущерб)
B) Reproducibility (Воспроизводимость)
C) **Exploitability (Исчерпаемость/Простота использования)**
D) Discoverability (Обнаруживаемость)

1. **Для выявления уязвимости «Path Traversal» наиболее эффективным методом динамического тестирования является:**

A) Статический анализ исходного кода
B) **Фаззинг-тестирование с подстановкой последовательностей ../ в параметры запроса**
C) Проверка контрольных сумм исполняемых файлов
D) Анализ прав доступа в Active Directory

1. **В системе классификации уязвимостей, что означает идентификатор CVE?**

A) Описание общих типов программных ошибок (Common Weakness Enumeration)
B) **Уникальный номер конкретной уязвимости в конкретном ПО (Common Vulnerabilities and Exposures)**
C) Метрика критичности уязвимости от 0 до 10
D) Протокол передачи данных о взломе

1. **Какое из перечисленных действий относится к этапу «D» (Dynamic) в тестировании безопасности?**

A) Проверка кода без его запуска инструментами SAST
B) **Анализ запущенного веб-приложения на наличие SQL-инъекций инструментами DAST**
C) Изучение нормативной базы ГОСТ Р 56939

D) Обфускация кода перед деплоем

1. **В рамках OWASP Top 10, какая категория описывает риски, связанные с использованием устаревших компонентов с известными дырами?**

A) Broken Access Control
B) Cryptographic Failures
C) **Vulnerable and Outdated Components**
D) Server-Side Request Forgery

Компетенция ОПК-15: Администрирование, контроль и мониторинг

1. **Какая технология позволяет безопасно передавать секреты (пароли, API-ключи) в контейнеризированные приложения Docker/K8s (Тема 13)?**

A) Прописывание паролей в переменные окружения в Dockerfile
B) **Использование специализированных хранилищ (HashiCorp Vault, Kubernetes Secrets)**
C) Хранение паролей в открытом виде в Git-репозитории
D) Передача секретов через незашифрованные HTTP-заголовки

1. **Основная задача SIEM-системы при мониторинге безопасности ПО — это:**

A) Автоматическое исправление ошибок в коде
B) **Сбор, корреляция событий из разных источников и выявление аномалий в реальном времени**
C) Резервное копирование баз данных
D) Шифрование жестких дисков серверов

1. **При администрировании API, какой механизм обеспечивает безопасную передачу прав доступа между сервисами без передачи пароля пользователя (Тема 11)?**

A) Базовая аутентификация (Login/Pass)
B) **Протокол OAuth 2.0 / JWT-токены**
C) Симметричное шифрование DES
D) Хранение сессий в Cookies без флага HttpOnly

1. **Что из перечисленного является обязательным требованием ФЗ-152 при обработке персональных данных в ПО ?**

A) Обязательная обфускация кода
B) **Обеспечение локализации баз данных на территории РФ и защита прав субъектов ПДн**
C) Использование только открытого исходного кода
D) Запрет на использование хеш-функций

1. **Инструментальный мониторинг защищенности в DevSecOps подразумевает:**

A) Проверку кода раз в год перед аттестацией
B) **Непрерывное сканирование образов и зависимостей в CI/CD пайплайне**
C) Только ручной аудит логов администратором
D) Отключение всех средств защиты для ускорения разработки

Компетенция ОПК-7.3: Анализ защищенности и верификация ПО

1. **Какая функция в языке C++ считается небезопасной и может привести к переполнению буфера (Тема 5)?**

A) strncpy()
B) **gets()**

1. C) printf("%s", str)

D) std::vector::at()


1774292621

1. **В чем заключается основное отличие статического анализа (SAST) от динамического (DAST)?**

A) SAST требует запуска программы, DAST — нет

B) **SAST анализирует исходный код или байт-код без запуска, DAST тестирует работающее приложение**

C) SAST ищет только ошибки в логике, DAST — только ошибки в синтаксисе

D) Между ними нет разницы

1. **При верификации криптографической защиты паролей, какой подход является наиболее надежным ?**

A) Шифрование алгоритмом AES-256 с хранением ключа в коде

B) Хеширование алгоритмом MD5

C) **Использование адаптивных функций хеширования (Argon2, bcrypt) с солью (salt)**

D) Хранение паролей в Base64

1. **Для чего применяется обфускация программного обеспечения?**

A) Для ускорения работы программы

B) **Для затруднения анализа алгоритмов и поиска уязвимостей методом реверс-инжиниринга**

1. C) Для автоматического исправления багов

D) Для сжатия размера исполняемого файла

1. **При анализе защищенности выявлено, что JWT-токен не имеет цифровой подписи (алгоритм "none"). К чему это может привести?**

A) К замедлению работы сервера

B) **К возможности подделки данных пользователя (Privilege Escalation) на стороне клиента**

C) К автоматическому шифрованию всех данных в БД

D) Ни к чему, это стандартная практика для экономии трафика

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-

педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Ложников, П. С. Средства безопасности операционной системы ROSA Linux : учебное пособие : [16+] / П. С. Ложников, А. О. Провоторский. – Омск : Омский государственный технический университет (ОмГТУ), 2017. – 94 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493349 (дата обращения: 17.04.2026). – Библиогр. в кн. – ISBN 978-5-8149-2502-2. – Текст : электронный.

2. Власенко, А. Ю. Операционные системы : учебное пособие : [16+] / А. Ю. Власенко, С. Н. Карабцев, Т. С. Рейн. – Кемерово : Кемеровский государственный университет, 2019. – 161 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574269 (дата обращения: 09.04.2026). – Библиогр. в кн. – ISBN 978-5-8353-2424-8. – Текст : электронный.

3. Куль, Т. П. Операционные системы : учебное пособие : [16+] / Т. П. Куль. – Минск : РИПО, 2019. – 312 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=599951 (дата обращения: 10.04.2026). – Библиогр. в кн. –

ISBN 978-985-503-940-3. – Текст : электронный.

4. Жидков, О. М. Сетевые операционные системы / О. М. Жидков. – Москва : Лаборатория книги, 2011. – 114 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=142238 (дата обращения: 14.04.2026). – ISBN 978-5-504-00184-5. – Текст : электронный.

5. Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие по дисциплине "Безопасность операционных систем" для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем" / А. Г. Киренберг ; Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, 2022. – 1 файл (1,48 Мб). – URL: http://library.kuzstu.ru/meto.php?n=91889&type=utchposob:common (дата обращения: 23.03.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Введение в операционные системы и основы программирования : учебно-методическое пособие / Г. П. Аверьянов, В. А. Будкин, В. В. Дмитриева, И. А. Кунов. — Москва : НИЯУ МИФИ, 2015. — 260 с. — ISBN 978-5-7262-1994-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/119473 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Сычев, О. А. Лабораторный практикум по дисциплине «Операционные системы». Клиент-серверные приложения : учебно-методическое пособие / О. А. Сычев, Е. Д. Беришева. — Волгоград : ВолгГТУ, 2019. — 64 с. — ISBN 978-5-9948-3440-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157227 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Сычев, О. А. Лабораторный практикум по дисциплине «Операционные системы». Управление процессами : учебно-методическое пособие / О. А. Сычев, Е. Д. Беришева. — Волгоград : ВолгГТУ, 2018. — 64 с. — ISBN 978-5-9948-3027-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157226 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. — Санкт-Петербург : Лань, 2020. — 120 с. — ISBN 978-5-8114-4192-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126937 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

5. Власенко, А. Ю. Операционные системы : учебное пособие / А. Ю. Власенко, С. Н. Карабцев, Т. С. Рейн. — Кемерово : КемГУ, 2019. — 161 с. — ISBN 978-5-8353-2424-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121996 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Безопасность операционных систем : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 46 с. – URL: http://library.kuzstu.ru/meto.php?n=4633 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Универсальная полнотекстовая база данных электронных периодических изданий «ИВИС» https://eivis.ru/

2. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/

3. Электронная библиотечная система «Лань» http://e.lanbook.com

4. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21

5. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv

6. Образовательная платформа «Юрайт» https://urait.ru/

7. Электронная библиотечная система «Znanium» https://new.znanium.com/my/documents

8. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm

9. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?

10. Национальная электронная библиотека https://rusneb.ru/

11. Электронная библиотека http://library.gorobr.ru/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646

2. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Безопасность программного обеспечения"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Безопасность программного обеспечения", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Ubuntu
2. Libre Office
3. Mozilla Firefox
4. Google Chrome

5. Yandex
6. 7-zip
7. Microsoft Windows
8. ESET NOD32 Smart Security Business Edition
9. Kaspersky Endpoint Security

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Безопасность программного обеспечения"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.