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

Программные решения по защите информации

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 "Программные решения по защите информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-2 - Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

-

Результаты обучения по дисциплине:

Знать программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

Уметь определять назначение программных средства.

Владеть навыками работы с программными средствами системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

2 Место дисциплины "Программные решения по защите информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: .

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 "Программные решения по защите информации" 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 "Программные решения по защите информации" составляет 7 зачетных единиц, 252 часа.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 4/Семестр 8			
Всего часов	252		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия			
Практические занятия	64		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	64		
Самостоятельная работа	56		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Программные решения по защите информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	**Трудоемкость в часах**
	ОФ
1. Современные парадигмы защиты информации: Zero Trust и Secure by Design и др.	2
2. API и микросервисы	2
3. Облачная безопасность и DevSecOps	2
4. Контейнеризация и Kubernetes	2
5. Архитектура безопасности и моделирование угроз	2
6. Безопасная разработка и SDLC	2
7. Криптография и управление ключами в ПО	2
8. Защита данных в пути и в покое	2
9. Тестирование безопасности ПО: SAST/DAST/IAST , тестирование API и др.	2
10. Управление удостоверениями и доступом	2
11. Мониторинг, инцидент-ответ и цифровая охрана	2
12. Безопасность цепочек поставок ПО и приватность	2
13. Безопасность облачных и cloud-native сред	4
14. Безопасность цепочек поставок ПО и приватная инфраструктура	4
Итого	**32**

4.2. Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
1.Работа с программными решениями по защите информации	64
Итого	**64**

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

Вид СРС	**Трудоемкость в часах**
	ОФ

Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	28
Оформление отчетов по практическим и(или) лабораторным работам	22
Подготовка к промежуточной аттестации	6
Итого	**56**
Самостоятельная работа под руководством преподавателя	64
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Программные решения по защите информации"

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-12	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	**Знать** программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. **Уметь** определять назначение программных средства. **Владеть** навыками работы с программными средствами системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	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:

1) Современные парадигмы защиты информации: Zero Trust и Secure by Design и др.

· Q1. MCQ. Каковы ключевые принципы модели Zero Trust? A) доверяй по умолчанию внутри сети; B) проверяй явно, применяй наименьшие привилегии, сегментацию, предполагаю взлом; C) полагайся только на VPN; D) полагайся на периметр сети. Правильный ответ: B

· Q2. Краткий ответ. Что означает концепция «постоянная проверка» в Zero Trust? Какие данные контекста учитываются при доступе? Кратко: каждое обращение к ресурсам проверяется, привилегии минимизированы, используется контекст (пользователь, устройство, география, время и т.д.).

· Q3. Кейс. Опишите, как внедрить принципы Zero Trust в архитектуру веб-приложения: какие компоненты сегментировать, как контролировать доступ, какие данные шифровать и как вести мониторинг. Желаемо указать: микро-санкционирование, непрерывную аутентификацию, атрибутный контроль, шифрование в пути и покое, аудит.

2) API и микросервисы

· Q1. MCQ. Какие методы защиты API являются современными и рекомендуемыми? A) API-ключи; B) OAuth 2.0 / OIDC; C) mTLS; D) все перечисленное. Правильный ответ: D

· Q2. Краткий ответ. В чем принципиальная разница между OAuth 2.0 и OpenID Connect (OIDC)? Кратко: OAuth 2.0 — протокол авторизации (права доступа к ресурсам); OIDC поверх OAuth 2.0 — добавляет аутентификацию и идентификатор пользователя (OIDC удостоверение).

· Q3. Кейс. Вы проектируете API-шлюз для набора микросервисов. Какие защитные механизмы и конфигурации вы бы включили (перечислить минимум 5 пунктов)? Примеры: аутентификация/авторизация через OAuth2/OIDC, mTLS между клиентом и шлюзом, API-ключи для сервисных вызовов, политика rate limiting и угроз-защита, мониторинг и аудит, секреты через безопасное хранилище, шифрование в покое и TLS в пути.

3) Облачная безопасность и DevSecOps

· Q1. MCQ. Что означает модель разделения ответственности в облаке (Shared Responsibility Model)? A) клиент отвечает за все аспекты; B) провайдер отвечает за все; C) ответственность делится между провайдером и заказчиком; D) ответственность переходит к внешнему аудиту. Правильный ответ: C

· Q2. Краткий ответ. Что такое policy-as-code? Приведите пример инструмента. Кратко: конфигурации и требования безопасности описываются в виде кода и автоматически применяются и валидируются; пример: OPA, Terraform with Sentinel, Open Policy Agent.

· Q3. Кейс. Опишите CI/CD конвейер с DevSecOps: какие этапы безопасности вставите в пайплайн и какие артефакты проверяете на каждом этапе. Пример: статический анализ кода (SAST) на коммитах, сканирование зависимостей на уязвимости, лаборатия контейнеров (образи), проверка конфигураций (IaC), динамический тест на pre-prod, ротация секретов, контроль изменений (policy-as-code), аудит и журналирование.


1774321435

4) Контейнеризация и Kubernetes

· Q1. MCQ. Что означает процесс сканирования образов контейнеров? A) анализ кода внутри образа; B) поиск известных CVE и уязвимостей в слоях образа; C) выполнение тестов производительности; D) верификация лицензий. Правильный ответ: B

· Q2. Краткий ответ. Какой подход лучше всего ограничивает east-west трафик в Kubernetes? Кратко: внедрение сетевых политик (NetworkPolicy) или Cilium/Istio с мерами фильтрации, принцип «default deny», использование сетевых тегов/лейблов.

· Q3. Кейс. Опишите набор защит для рантайма Kubernetes: контроль доступа к API-серверу, сканирование образов, модули безопасности (PSP/OPA Gatekeeper), мониторинг поведения подов. Включить: RBAC/ABAC для API, запрещение сетевых открытых портов, подмодули без привилегий, секреты в зашифрованном хранилище, жаркие правила аудита.

5) Архитектура безопасности и моделирование угроз

· Q1. MCQ. Что представляет собой STRIDE в threat modeling? A) набор сетевых политик; B) методология угроз: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege; C) стандарт кода; D) метод тестирования. Правильный ответ: B

· Q2. Краткий ответ. Опишите основные этапы threat modeling для нового сервиса. Кратко: определить контекст/границы системы, построить диаграмму архитектуры, перечислить угрозы по STRIDE, оценить риски, разработать меры смягчения и повторно проверить.

· Q3. Кейс. Выберите архитектурные паттерны защиты (defense-in-depth, least privilege, segmentation) и обоснуйте их применение к данному сценарию с несколькими микросервисами. Пример: многослойная аутентификация, изоляция данных, шифрование, контроль доступа на уровне сервисов, мониторинг, ретроактивная защита.

6) Безопасная разработка и SDLC

· Q1. MCQ. Какой пункт не относится к Secure SDLC? A) требования безопасности на стадии планирования; B) безопасное кодирование и тестирование; C) игнорирование уязвимостей до релиза; D) внедрение контроля изменений. Правильный ответ: C

· Q2. Краткий ответ. Как проследить безопасность требований через user stories и тесты? Кратко: формулировать безопасные критерии приемки, связывать их с тест-кейсам, трассировать через backlog и репозитории, использовать чек-листы безопасности.

· Q3. Кейс. Приведите пример приоритизации уязвимостей в рамках спринта: как выбрать, какие исправлять в первую очередь, на что опираться (риски, влияние, сложность, зависимость от внешних компонентов). Включить: классификация по CVSS, бизнес-риски, критичность сервиса, время устранения, влияние на клиента.

7) Криптография и управление ключами в ПО

· Q1. MCQ. Что лучше использовать для целостности данных: хеш-функцию или подпись? A) хеш-функцию; B) подпись; C) neither; D) обе в зависимости от контекста. Правильный ответ: D (для целостности и аутентичности данные часто подписываются, хеши могут использоваться для быстрого сравнения).

· Q2. Краткий ответ. В чем разница между симметричным и асимметричным шифрованием? Приведите пример. Кратко: симметричное — один ключ (AES); асимметричное — пара ключей (например, RSA, ECC). Примеры: AES — симметричное; RSA/ECC — асимметричное.

· Q3. Кейс. Опишите безопасное управление ключами: создание, хранение, ротация, аварийное восстановление, аудит доступа к ключам в облаке (KMS/HSM). Включить требования к срокам ротации, хранение в HSM/Vault, многофакторный доступ к ключам, журнал изменений.

8) Защита данных в пути и в покое

· Q1. MCQ. Какие преимущества TLS 1.3 по сравнению с TLS 1.2? A) упрощённая рукопожатие, поддержка PFS, 0-RTT; B) меньше поддержки криптоалгоритмов; C) больше задержек; D) нет преимуществ. Правильный ответ: A

· Q2. Краткий ответ. Какие подходы используют для защиты данных в покое в базе данных? Кратко: шифрование столбцов, Transparent Data Encryption (TDE), ключи мастер-ключей, управление ключами, безопасное хранение ключей (KMS/HSM).

· Q3. Кейс. Опишите настройки TLS в веб-сервисе (версия TLS, каналы, конфигурации: протоколы, cipher suites, PFS, 0-RTT и т.д.) и как проверить их соответствие рекомендациям безопасности. Включить: отключение TLS 1.0/1.1, использование TLS 1.3, строгую настройку cipher suites, certificate pinning там, где уместно; тесты конфигураций (SSL Labs, tomcat/nginx конфиги).

9) Тестирование безопасности ПО: SAST/DAST/IAST, тестирование API и др.

· Q1. MCQ. Какое утверждение верно? A) SAST — анализ кода во время выполнения; B) DAST — анализ внешнего поведения приложения в реальном времени; C) IAST — внутренний статический

анализ кода; D) Все неверно. Правильный ответ: B

· Q2. Краткий ответ. Что такое fuzzing и когда его применять? Кратко: автоматизированное подбивание входных данных до краха/уязвимости; применяется на фазе тестирования API, сериализаторов, протоколов.

· Q3. Кейс. Сформируйте базовый тест-план для API: какие типы тестов включить (SAST, DAST, IAST, тесты контрактов, fuzzing), как организовать результаты и цикл исправления. Включить критерии приемки по безопасности, требования к окружению, частоту повторных запусков, метрики.

10) Управление удостоверениями и доступом

· Q1. MCQ. Что означает RBAC и ABAC? A) RBAC — управление доступом на основе ролей; ABAC — на основе атрибутов; B) RBAC — абстрактная база доступа; C) ABAC — только для облака; D) RBAC — только для файлов. Правильный ответ: A

· Q2. Краткий ответ. Какие MFA методы существуют и почему они важны? Кратко: одноразовые коды (TOTP/HOTP), push-уведомления, биометрия; повышают уровень защиты от компрометации паролей.

· Q3. Кейс. Опишите пример проектирования управления доступом для облачного приложения: роли, политики ABAC/RBAC, условия доступа, журналирование и аудит. Включить: принцип наименьших привилегий, многофакторную авторизацию для чувствительных операций, временные ключи/права доступа.

11) Мониторинг, инцидент-ответ и цифровая охрана

· Q1. MCQ. Какова роль MITRE ATT&CK в мониторинге и IR? A) набор инструментов сетевого сканирования; B) база знаний техник атак и контрмер; C) система управления версиями; D) инструмент тестирования производительности. Правильный ответ: B

· Q2. Краткий ответ. Приведите пример детекции инцидента: что может сигнализировать о компрометации? Кратко: аномальные входы в учетную запись, необычные геолокации, неожиданные требования к доступу, нестандартные процессы.

· Q3. Кейс. Опишите план инцидент-ответ (IR playbook) для кейса: обнаружено необычное сетевое соединение на сервере. Какие шаги, роли, коммуникации и дальнейшие действия? Включить: инцидент identification, containment, eradication, recovery, lessons learned, коммуникации внутри компании, уведомления.

12) Безопасность цепочек поставок ПО и приватность

· Q1. MCQ. Что такое SBOM? A) документ, описывающий цепочку поставки ПО и все зависимости; B) стандарт аудита кода; C) серверная конфигурация; D) метод тестирования уязвимостей. Правильный ответ: A

· Q2. Краткий ответ. Как SBOM помогает управлять уязвимостями и комплаенсом? Кратко: позволяет выявлять уязвимости в зависимостях, отслеживать обновления, документировать состав ПО для аудита.

· Q3. Кейс. Опишите кейс аудита зависимости проекта: какие шаги, какие данные собираются, как выбираются обновления и как документируется соответствие требованиям приватности. Включить: сбор SBOM (SPDX/CycloneDX), анализ зависимостей на уязвимости, план обновления, журнал изменений, политика приватности и минимизации данных.

13) Безопасность облачных и cloud-native сред

· Q1. MCQ. Какие основные практики безопасности cloud-native? A) IAM в облаке, шифрование, мониторинг и логирование; B) только виртуальные машины; C) полная открытость конфигураций; D) отсутствие политики управления секретами. Правильный ответ: A

· Q2. Краткий ответ. Как Kubernetes обеспечивает безопасность в облаке и в cloud-native среде (упомянуть PSO/OPA Gatekeeper)? Кратко: контролем доступа к API, политики безопасности (OPA Gatekeeper), ограничение привилегий подов, управление секретами, безопасность образов, сетевые политики.

· Q3. Кейс. Спроектируйте безопасное cloud-native приложение: какие элементы (IAM, секреты, конфигурации, политики, мониторинг) вы внедрите и как будете обеспечивать непрерывность безопасности в CI/CD. Включить: policy-as-code, секрет-менеджмент, сканирование образов, безопасную конфигурацию инфраструктуры, мониторинг и уведомления.

14) Безопасность цепочек поставок ПО и приватная инфраструктура

· Q1. MCQ. Какой подход лучше для управления безопасностью в приватной инфраструктуре? A) полагаться на внешние репозитории без SBOM; B) использовать SBOM, политики изменения, аудит зависимостей; C) игнорировать обновления; D) открывать все порты. Правильный ответ: B

· Q2. Краткий ответ. Какие меры контроля изменений применяются в приватной

инфраструктуре? Кратко: инфраструктура как код с проверками (IaC), политики код-ревью, подпись артефактов, управление секретами, мониторинг изменений, журнал аудита.

· Q3. Кейс. Опишите сценарий обеспечения защиты приватной инфраструктуры: сетевые сегменты, доступ к системам, безопасное обновление образов и зависимостей, аудит. Включить: ограничение доступа по ролям, секреты в закрытых хранилищах, шифрование трафика, автоматизированные обновления и безопасный процесс выпуска.

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:

о пройденное тестирование.

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

На экзамене обучающийся отвечает 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 на экзамен:

MCQ. Каковы ключевые принципы модели Zero Trust? A) доверяй по умолчанию внутри сети; B) проверяй явно, применяй наименьшие привилегии, сегментацию, предполагаю взлом; C) полагайся только на VPN; D) полагайся на периметр сети.

MCQ. Какие методы защиты API являются современными и рекомендуемыми? A) API-ключи; B) OAuth 2.0 / OIDC; C) mTLS; D) все перечисленное. Правильный ответ: D

MCQ. Что означает модель разделения ответственности в облаке (Shared Responsibility Model)? A) клиент отвечает за все аспекты; B) провайдер отвечает за все; C) ответственность делится между провайдером и заказчиком; D) ответственность переходит к внешнему аудиту. Правильный ответ: C

MCQ. Что означает процесс сканирования образов контейнеров? A) анализ кода внутри образа; B) поиск известных CVE и уязвимостей в слоях образа; C) выполнение тестов производительности; D) верификация лицензий. Правильный ответ: B

MCQ. Что представляет собой STRIDE в threat modeling? A) набор сетевых политик; B)

методология угроз: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege; C) стандарт кода; D) метод тестирования. Правильный ответ: B

MCQ. Какой пункт не относится к Secure SDLC? A) требования безопасности на стадии планирования; B) безопасное кодирование и тестирование; C) игнорирование уязвимостей до релиза; D) внедрение контроля изменений. Правильный ответ: C

MCQ. Что лучше использовать для целостности данных: хеш-функцию или подпись? A) хеш-функцию; B) подпись; C) neither; D) обе в зависимости от контекста. Правильный ответ: D (для целостности и аутентичности данные часто подписываются, хеши могут использоваться для быстрого сравнения).

MCQ. Какие преимущества TLS 1.3 по сравнению с TLS 1.2? A) упрощённая рукопожатие, поддержка PFS, 0-RTT; B) меньше поддержки криптоалгоритмов; C) больше задержек; D) нет преимуществ. Правильный ответ: A

MCQ. Какое утверждение верно? A) SAST — анализ кода во время выполнения; B) DAST — анализ внешнего поведения приложения в реальном времени; C) IAST — внутренний статический анализ кода; D) Все неверно. Правильный ответ: B

MCQ. Что означает RBAC и ABAC? A) RBAC — управление доступом на основе ролей; ABAC — на основе атрибутов; B) RBAC — абстрактная база доступа; C) ABAC — только для облака; D) RBAC — только для файлов. Правильный ответ: A

MCQ. Какова роль MITRE ATT&CK в мониторинге и IR? A) набор инструментов сетевого сканирования; B) база знаний техник атак и контрмер; C) система управления версиями; D) инструмент тестирования производительности. Правильный ответ: B

MCQ. Что такое SBOM? A) документ, описывающий цепочку поставки ПО и все зависимости; B) стандарт аудита кода; C) серверная конфигурация; D) метод тестирования уязвимостей. Правильный ответ: A

MCQ. Какие основные практики безопасности cloud-native? A) IAM в облаке, шифрование, мониторинг и логирование; B) только виртуальные машины; C) полная открытость конфигураций; D) отсутствие политики управления секретами. Правильный ответ: A

MCQ. Какой подход лучше для управления безопасностью в приватной инфраструктуре? A) полагаться на внешние репозитории без SBOM; B) использовать SBOM, политики изменения, аудит зависимостей; C) игнорировать обновления; D) открывать все порты. Правильный ответ: B

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. Петухов, В. И. Проблемы реинжиниринга российских предприятий / В. И. Петухов. – Москва ; Берлин : Директ-Медиа, 2014. – 59 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=256310 (дата обращения: 15.04.2026). – Библиогр. в кн. – ISBN 978-5-4475-3063-1. – DOI 10.23681/256310. – Текст : электронный.

2. Власова, Н. О. Реинжиниринг бизнес-процессов с использованием информационных технологий : выпускная квалификационная работа по программе бакалавриата / Н. О. Власова ; Юго-Западный государственный университет, Кафедра региональной экономики и менеджмента. – Курск : б.и., 2017. – 84 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=463008 (дата обращения: 16.04.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Золотарёв, О. В. Использование ИТ в реинжиниринге бизнес-процессов : методические указания / О. В. Золотарёв. — Москва : РосНОУ, 2015. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/162174 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Новикова, В. Н. Практикум по моделированию и реинжинирингу бизнес-процессов : учебное пособие / В. Н. Новикова, С. В. Ратафьев, Г. И. Белявский. — Нижний Новгород : НГТУ им. Р. Е. Алексеева, 2020. — 158 с. — ISBN 978-5-502-01405-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/260219 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Крамарь, А. В. Реинжиниринг и автоматизация процессов управления маркетинговой деятельностью (на примере ОАО «Брянский молочный комбинат») / А. В. Крамарь ; Брянский государственный технический университет. – Брянск : б.и., 2020. – 75 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=597789 (дата обращения: 10.04.2026). – Текст : электронный.

6.3 Методическая литература

1. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И. Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: http://library.kuzstu.ru/meto.php?n=553 (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 "Программные решения по защите информации"

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 "Программные решения по защите информации", 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. Opera
6. 7-zip
7. Open Office
8. Microsoft Windows
9. ESET NOD32 Smart Security Business Edition
10. Kaspersky Endpoint Security

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Программные решения по защите информации"

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.