Приложение ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2021-2022 уч.г.:
Комплект контрольно-оценочных средств по
ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект контрольно-оценочных средств

по

ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2021

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553.

Составитель:
Косинова И.В., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами, которые соотнесены с требуемыми результатами освоения образовательной программы (компетенциями выпускников). Совокупность запланированных результатов обучения должна обеспечивать выпускнику освоение всех общих компетенций (далее – ОК), профессиональных компетенций (далее – ПК), установленных ФГОС СПО.

Контрольно-оценочные средства (далее - КОС)***1*** предназначены для контроля и оценки образовательных достижений обучающихся по ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами**.**

КОС включают типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и практического опыта, характеризующих этапы формирования компетенций в процессе освоения образовательной программы для организации промежуточной аттестации в форме **экзамена по модулю**.

КОС разработан на основании рабочей программы ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.2 Планируемые результаты освоения профессионального модуля:

Предметом оценки служат знания, умения и практический опыт, предусмотренные ФГОС СПО, направленные на формирование профессиональных компетенций.

Таблица 1***2***

Наименование МДК и практик	Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/знания/умения/ практический опыт
МДК 02.01 Программные и программно-аппаратные средства защиты информации	Экзаменационная работа	ПК 2.1, З1-З9, У1-У6, ПО1-ПО9; ПК 2.2, З1-З14, У1-У10, П1-П3; ПК 2.3, З1-З12, У1-У10, П1-П2
МДК 02.02. Криптографические средства защиты информации		
УП.02 Учебная практика		

1 КОС должен соответствовать ФГОС, ПРИМЕРНОЙ ПРОГРАММЕ И РАБОЧЕЙ ПРОГРАММЕ

2 Компоненты ПМ взять из РУП

ПП.02 Производственная практика		

В результате освоения профессионального модуля обучающийся должен **уметь**:

У1. применять технические средства для криптографической защиты информации конфиденциального характера;

У2. применять технические средства для уничтожения информации и носителей информации;

У3. применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4. применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5. применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6. применять инженерно-технические средства физической защиты объектов информатизации.

В результате освоения профессионального модуля обучающийся должен **знать**:

З1. порядок технического обслуживания технических средств защиты информации;

З2. номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3. физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

З4. порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5. методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6. номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7. основные принципы действия и характеристики технических средств физической защиты;

З8. основные способы физической защиты объектов информатизации;

З9. номенклатуру применяемых средств физической защиты объектов информатизации.

В результате освоения профессионального модуля обучающийся должен **иметь практический опыт:**

ПО1. установки, монтажа и настройки технических средств защиты информации;

ПО2. технического обслуживания технических средств защиты информации;

ПО3. применения основных типов технических средств защиты информации;

ПО4. выявления технических каналов утечки информации;

ПО5. участия в мониторинге эффективности технических средств защиты информации;

ПО6. диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

ПО7. проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

ПО8. проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

ПО9. установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

Профессиональные и общие компетенции, которые формируются при изучении профессионального модуля:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Планируемые личностные результаты освоения рабочей программы профессионального модуля:

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.3 Контроль и оценка результатов освоения профессионального модуля

Таблица 2

Код и наименование профессиональных и общих компетенций, формируемые в рамках междисциплинарного курса	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Тестирование, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения профессионального модуля для организации промежуточной аттестации в форме экзамена

2.1. Тестовые задания

Вариант 1

Задание №1. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие основные виды документов разрабатываются в рамках инженерно-технической защиты информации? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) Технические паспорта, инструкции по эксплуатации

б) Политики безопасности, регламенты, инструкции

в) Финансовые отчёты, бизнес-планы

г) Учебные пособия, справочники

Задание №2. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие этапы включает процесс разработки документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) Анализ требований, разработка структуры документа, согласование, утверждение

б) Закупка оборудования, монтаж, тестирование

в) Составление бюджета, финансовый контроль, отчётность

г) Рекрутинг персонала, обучение, аттестация

Задание №3. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

Какие требования предъявляются к оформлению и структуре основных документов по ИТЗИ?

а) Наличие титульного листа, оглавления, разделов с описанием политики, процедур, инструкций

б) Форматирование текста, шрифты, отступы

в) Ссылки на сторонние ресурсы, иллюстрации

г) Использование цветных схем, диаграмм

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

Какие типовые ошибки могут быть допущены при разработке документации и как их избежать?

а) Неправильное оформление, отсутствие согласования с заинтересованными сторонами
б) Несоответствие стандартам, отсутствие обновлений
в) Недостаточная детализация, неполнота описания процедур

Задание №5. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие критерии используются для оценки качества разработанной документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: 31, 32, У 4, ПК. 2.2, ПК.2.3)***

а) Соответствие стандартам, полнота охвата всех аспектов ИТЗИ
б) Простота восприятия, удобство использования
в) Скорость разработки, стоимость
г) Частота обновлений, доступность для пользователей

Задание №6. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие уровни защиты применяются в системах программной и программно-аппаратной защиты информации?

а) Аппаратный уровень, сетевой уровень, прикладной уровень.
б) Уровень операционной системы, уровень приложений, уровень пользователей.
в) Уровень управления доступом, уровень шифрования, уровень аутентификации.
г) Все вышеперечисленное.

Задание №7. В задании установите соответствие между видом аспектом его решением. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.

При разработке комплекса мер по обеспечению программной и программно-аппаратной защиты информации, возможные следующие решения. Сопоставьте аспекты с соответствующими его решениями.

1. Аутентификация и авторизация:	а) Настройка политик контроля доступа (ACLs) для каждого ресурса.
2. Шифрование:	б) Установка систем мониторинга и анализа событий безопасности (SIEM).
3. Контроль доступа:	в) Шифрование данных на всех уровнях передачи и хранения.
4. Мониторинг и обнаружение угроз:	г) Проведение тренингов по вопросам информационной безопасности для всех сотрудников
5. Резервное копирование и восстановление:	д) Создание регулярных резервных копий данных.
6. Обучение персонала:	е) Использование многофакторной аутентификации (MFA) для всех учетных записей сотрудников.

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание №8. Прочитайте ситуационную задачу и определите верные действия. Обведите кружочком номер правильного ответа.

Компания использует несколько серверов для хранения данных, приложения работают в облачной среде, а сотрудники используют корпоративные ноутбуки для работы. Необходимо обеспечить защиту данных компании как на уровне программного обеспечения, так и аппаратного уровня. Что войдет в комплекс мер по обеспечению программной и программно-аппаратной защиты информации:

1. Защита от несанкционированного доступа.
2. Обеспечение конфиденциальности данных.
3. Поддержание целостности данных.
4. Обнаружение и предотвращение возможных угроз.
5. Все перечисленное.

Задание №9. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа

Какой международный стандарт описывает требования к системам менеджмента информационной безопасности? ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***

а) ISO 27001
б) ISO 9001
в) ISO 14001
г) OHSAS 18001

Задание №10. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.

Вам необходимо разработать политику информационной безопасности, и план внедрения стандартов безопасности, который будет соответствовать международным требованиям и учитывать специфику деятельности компании. ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***.
Выберите следующие аспекты и расположите их последовательно:

1. Процессы и процедуры
2. Ресурсы и обучение
3. Оценка эффективности:
4. Выбор стандарта безопасности
5. Интеграция с существующими системами

1	
2	
3	
4	
5	

Задание №11. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. Обведите кружочком номер правильного ответа. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу. ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***

1. Выбор стандарта безопасности	а) Отслеживание изменений в инфраструктуре, процессах и отделах
2. Процессы и процедуры	б) Назначенные ответственные лица для работы с программой обучения и привлечение внешних консультантов
3. Процедура управления изменениями	в) Процесс управления рисками и регулярный мониторинг и аудит систем безопасности
4. Ресурсы и обучение	г) Пилотные проекты, риски: согласование с бизнес-процессами, несовместимость систем.
5. Оценка эффективности	д) Проводить методы оценки: Внутренние и внешние аудиты, мониторинги
6. Интеграция с существующими системами	е) Определить наиболее подходящий стандарт(ы) безопасности.

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание №12. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие компоненты включаются в состав защищённой автоматизированной системы? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***

а) Серверы, рабочие станции, сетевое оборудование

б) Системы резервного копирования, антивирусное ПО, межсетевые экраны

в) Всё перечисленное

г) Только серверы и рабочие станции

Задание №13. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие уровни защиты информации обычно предусматриваются в защищённых автоматизированных системах? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***
а) Физический, административный, технический
б) Локальный, региональный, федеральный
в) Внешний, внутренний, смешанный
с) Открытый, закрытый, ограниченный

Задание №14. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие средства аутентификации обычно используются в защищённых автоматизированных системах? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***
а) Пароли, токены, биометрические данные
б) Логины, сертификаты, ключи доступа
в) Все перечисленные варианты
г) Только пароли и токены

Задание №15. Прочитайте ситуационную задачу и установите последовательность. Правильную последовательность запишите в таблицу
Вам необходимо разработать план мероприятий по защите автоматизированной системы от потенциальных угроз. ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3).***
Необходимо следующие аспекты расположить последовательно:

1. Меры по защите от несанкционированного доступа
2. Шифрование и аутентификация
3. Обучение персонала
4. План реагирования на инциденты
5. Анализ уязвимостей
6. Мониторинг и обнаружение аномалий

1	
2	
3	
4	
5	
6	

Задание №16. Прочитайте текст и впишите пропущенное слово в предложение. ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

….. воздействие – это воздействие, приводящее к нарушению нормального

функционирования объекта
Запишите ответ:

Задание № 17. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

1. Какой тип дестабилизирующего воздействия может привести к утечке конфиденциальной информации? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

а) Химическое
б) Биологическое
в Информационное
г) Психологическое

Задание № 18. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

2. Что из перечисленного не относится к мерам по защите от дестабилизирующих воздействий? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

а) Регулярное обновление программного обеспечения
б) Установка фильтров для воды
в) Обучение сотрудников правилам поведения в чрезвычайных ситуациях
г) Планирование корпоративного отдыха

Задание № 19. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.

3. Необходимо разработать комплексный план по выявлению, оценке и нейтрализации дестабилизирующих воздействий на объекты защиты компании. ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3).***

Определите последовательность разделов, которые должен быть включены в план:

1. Анализ уязвимостей
2. Обучение и повышение квалификации персонала
3. Организация мониторинга и реагирования
4. Разработка мер защиты
5. Идентификация и классификация угроз

Запишите ответ:

1	
2	
3	
4	

5	

4. **Задание № 20. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.** ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

1. Идентификация и классификация угроз:	а) Предложение программы обучения по ИБ, тренинги по реагированию и отработка необходимых навыков с системами мониторинга
2. Анализ уязвимостей	б) Организация системы мониторинга журналов событий и выполнение порядка действий реагирование
3. Разработка мер защиты:	в) Определение физической , технической защиты и Повышение устойчивости шифрования
4. Организация мониторинга и реагирования	г) Определение основных уязвимости=ей и методов анализа рисков
5. Обучение и повышение квалификации персонала	д) Определение видов угроз и рассмотрение критериев классификации угроз.

Запишите ответ:

1	
2	
3	
4	
5	

Задание №21. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие принципы входят в основу программно-аппаратной защиты информации? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

а) Минимальная достаточность прав доступа, разделение полномочий, контроль целостности

б) Доступность, конфиденциальность, целостность

в) Аутентификация, авторизация, аудит

г) Все вышеперечисленные

Задание №22. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какие устройства могут использоваться для аппаратной защиты информации? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

а) Межсетевые экраны (firewalls), криптографические процессоры, датчики

движения
б) Антивирусы, брандмауэры, прокси-серверы
в) Средства контроля доступа, серверы аутентификации, камеры наблюдения
г) Все вышеперечисленные

Задание №23. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие методы используются для программной защиты информации? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
а) Шифрование, аутентификация, контроль доступа
б) Резервное копирование, восстановление данных, архивирование
в) Анализ уязвимостей, тестирование на проникновение, патч-менеджмент

Задание №24. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие преимущества имеет программно-аппаратный комплекс защиты перед чисто программными решениями? ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***
а) Все пеперечисленное
б) Возможность интеграции различных уровней защиты
в) Упрощенное управление и администрирование
г) Более высокая надежность благодаря физической защите

Задание №25. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.
При разработке плана мероприятий по улучшению программно-аппаратной защиты информации от несанкционированного доступа, необходимо выполнить установку последовательность аспектов ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***:
1.Оценка эффективности
2. Разработка комплекса мер
3. Определение приоритетов
4.Планирование внедрения
5. Анализ текущего состояния системы защиты
Запишите ответ:

1	
2	
3	
4	
5	

Вариант 2

Задание №1. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие нормативные документы и стандарты регулируют разработку документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) ГОСТ Р 51583-2014, ГОСТ Р 51624-2000
б) ISO 9001, ISO 14001
в) СанПиН 2.2.4.548-96, СНиП 2.04.05-91
г) ГОСТ Р 57188-2016, ГОСТ Р 58082-2018

Задание №2. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие специалисты привлекаются к процессу разработки документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) Инженеры-электрики, программисты
б) Юристы, экономисты
в) Специалисты по ИТЗИ, аудиторы
г) Маркетологи, рекламщики

Задание №3. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие методологические подходы используются при разработке документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) Процессный подход, риск-ориентированный подход
б) Agile, Scrum
в) Lean Six Sigma, Kaizen d
г) SWOT-анализ, PESTEL-анализ

Задание №4. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие современные технологии и программные средства применяются для автоматизации процесса разработки документации по ИТЗИ? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) MS Office, Google Docs
б) Atlassian Confluence, SharePoint
в) AutoCAD, SolidWorks
г) SAP ERP, Oracle E-Business Suite

Задание №5. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
.Какие мероприятия проводятся после утверждения документации для её внедрения и сопровождения? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

а) Обучение персонала, аудит, мониторинг
б) Разработка новой версии документа, архивирование старой
в) Продажа документации третьим лицам, лицензирование
г) Создание дубликатов, перевод на другие языки

Задание №6. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что такое межсетевой экран (firewall)? ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***
а) Устройство или программа, контролирующая входящий и исходящий трафик на основе заранее установленных правил.
б) Метод шифрования данных.
в) Процесс проверки подлинности пользователя или устройства.
г) Система обнаружения вторжений.

Задание №7. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.

При разработке комплекса мер по обеспечению программной и программно-аппаратной защиты информации, возможные следующие решения. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3)***

1. Аутентификация и авторизация:	а) Разработка плана восстановления после инцидента
2. Шифрование:	б) Регулярное обновление и пересмотр прав доступа.
3. Контроль доступа:	в) Ограничение доступа к критически важным данным только для тех сотрудников, которым это действительно необходимо.
4. Мониторинг и обнаружение угроз:	г) Проведение регулярных тестов на проникновение (penetration testing).
5. Резервное копирование и восстановление:	д). Использование современных алгоритмов шифрования (AES, RSA).
6. Обучение персонала:	е) Инструктаж по распознаванию фишинговых атак и других социальных инженерных методов.

Запишите ответ:

1	
2	
3	
4	
5	

Задание №8. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.

Компания использует несколько серверов для хранения данных, приложения работают в облачной среде, а сотрудники используют корпоративные ноутбуки для работы. Необходимо обеспечить защиту данных компании как на уровне программного обеспечения, так и аппаратного уровня. ***(оцениваемые знания, умения, компетенции: З1, З2, У 4, ПК. 2.2, ПК.2.3).***

В комплекс мер по обеспечению программной и программно-аппаратной защиты информации должны войти следующие аспекты:

1. Аппаратные средства::	а) Политика, ограничивающие использование личных устройств для рабочих целей и обязательное использование MDM-решений для корпоративных устройств.
2. Управление обновлениями:	б) Межсетевые экраны (Firewalls), Устройства предотвращения вторжений
3. Защита мобильных устройств:	в) Автоматическая система установки обновлений и патчей и периодическое тестирование совместимости обновлений перед развертыванием.

Запишите ответ:

1	
2	
3	

Задание №9. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.

Какой стандарт относится к управлению информационной безопасностью в облачных сервисах? ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***

а) ISO 27017
б) ISO 27002
в) ISO 27701
г) ISO 50001

Задание №10. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа

Какой стандарт устанавливает требования к конфиденциальности персональных данных? ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***

а) GDPR
б) HIPAA

в) SOX
г) GLBA

Задание №11. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа
Какой стандарт является основой для оценки и сертификации систем управления информационной безопасностью? ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***
а) ISO 27006
б) ISO 10007
в) ISO 90003
с) ISO 31010

Задание №12. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.
Вам необходимо разработать план внедрения стандартов безопасности, который будет соответствовать международным требованиям и учитывать специфику деятельности вашей компании. ***(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК. 2.2, ПК.2.3)***. Рассмотрите следующие аспекты и укажите соответствие действия

1.Выбор стандарта безопасности	а) Процесс управления рисками и регулярный мониторинг и аудит систем безопасности
2.Процессы и процедуры	б) Отслеживание изменений в инфраструктуре, процессах и отделах
3.Процедура управления изменениями	в) Определить наиболее подходящий стандарт(ы) безопасности.
4. Ресурсы и обучение	г) Назначенные ответственные лица для работы с программой обучения и привлечение внешних консультантов
5.Оценка эффективности	д) Пилотные проекты, риски: согласование с бизнес-процессами, несовместимость систем
6.Интеграция с существующими системами	е) Проводить методы оценки: Внутренние и внешние аудиты, мониторинги

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание №13. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа
Что является основным назначением межсетевого экрана (firewall) в защищённых автоматизированных системах?
а) Обеспечение бесперебойной работы системы
б) Защита от несанкционированного доступа извне
в) Резервное копирование данных
г) Антивирусная защита

Задание №14. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа Какой стандарт регулирует требования к системам менеджмента информационной безопасности?
а) ISO 9001
б) ISO 27001
в) ISO 14001
г) ISO 45001

Задание №15. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа
Какое программное обеспечение используется для защиты от вредоносных программ в защищённых автоматизированных системах?
а) Межсетевые экраны
б) Антивирусы
в) Системы резервного копирования
г) Брандмауэры

Задание №16. Выберите правильный вариант ответа и обведите кружочком букву правильного ответ
Какие меры защиты данных предусмотрены в защищённых автоматизированных системах?
а) Шифрование, резервное копирование, контроль доступа
б) Регулярное обновление ПО, обучение сотрудников, использование антивирусного ПО
в) Всё перечисленное
г) Только шифрование и резервное копирование

Задание №17. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.
Для разработки плана мероприятий по улучшению программно-аппаратной защиты информации от несанкционированного доступа необходимо сопоставить этапы разработки с понятиями. ***(оцениваемые знания, умения, компетенции: У4, З1, З6, З3 , ПК. 2.2)***

1. Анализ текущего состояния	а) Методы оценки: регулярные аудиты,

системы защиты:	тестирование на проникновение, опросы сотрудников.
2. Определение приоритетов:.	б) Ресурсы: финансирование, квалифицированный персонал, современные технологии.
3. Разработка комплекса мер:	в) Аппаратные средства: установка межсетевых экранов, использование HSM-модулей для управления ключами шифрования.
4. Планирование внедрения:	г) Наибольшие угрозы: фишинговые атаки, взлом паролей, вредоносное ПО. Наиболее ценные данные: персональные данные клиентов, финансовые отчеты
5. Оценка эффективности:	д) Компоненты: серверы баз данных, рабочие станции сотрудников, сетевое оборудование.

Запишите ответ:

1	
2	
3	
4	
5	

Задание №18. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие основные виды дестабилизирующих воздействий существуют? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***
а) Физические, химические, биологические
б) Механические, электромагнитные, климатические
в) Информационные, психологические, экономические
г) Все вышеперечисленные

Задание №19. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Какие меры принимаются для минимизации последствий дестабилизирующих воздействий? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***
а) Установка систем видеонаблюдения
б) Создание резервных копий данных
в) Проведение регулярных тренировок персонала
г) Все вышеперечисленное

Задание №20. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Каким образом можно предотвратить дестабилизирующие воздействия на информационные системы? ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***
а) Все перечисленные методы
б) Применение межсетевых экранов
в) Шифрование данных
г) Использование антивирусного ПО

Задание №21. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.
Вам необходимо разработать план мероприятий по защите автоматизированной системы от потенциальных угроз. Учтите следующие аспекты. Рассмотрите следующие аспекты и укажите соответствие действия. ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

1. Идентификация и классификация угроз	а) Определение физической , технической защиты и Повышение устойчивости шифрования
2. Анализ уязвимостей	б) Определение основных уязвимостей и методов анализа рисков
3. Разработка мер защиты	в) Определение видов угроз и рассмотрение критериев классификации угроз.
4. Организация мониторинга и реагирования	г) Предложение программы обучения по ИБ, тренинги по реагированию и отработка необходимых навыков с системами мониторинга
5. Обучение и повышение квалификации персонала	д) Организация системы мониторинга журналов событий и выполнение порядка действий реагирование

Запишите ответ:

1	
2	
3	
4	
5	

Задание №22. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что представляет собой аппаратная защита информации? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***

а) Программное обеспечение для шифрования данных
б) Устройства и оборудование, обеспечивающие физическую безопасность информационных систем
в) Системы управления доступом
с) Методы обучения пользователей правилам безопасности

Задание №23. Прочитайте текст и впишите пропущенное слово в предложение. ***(оцениваемые знания, умения, компетенции: З1, У4, У5 , У10, ПК. 2.2, ПК.2.3)***

….. воздействие – это воздействие, приводящее к нарушению нормального функционирования объекта
Запишите ответ:

Задание №24. Выберите правильный вариант ответа и обведите кружочком букву правильного ответа.
Что такое принцип разделения полномочий? ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***
а) в
б) Ограничение возможности одного пользователя совершать критичные действия без согласования с другим пользователем
в) Распределение ресурсов между пользователями
г) Запрещение доступа ко всей информации одновременно

Задание №25. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.

При разработке плана мероприятий по улучшению программно-аппаратной защиты информации от несанкционированного доступа, необходимо выполнить установку последовательность аспектов ***(оцениваемые знания, умения, компетенции: З2, З3, У1, У4 ПК. 2.2, ПК.2.3)***:

1. Определение приоритетов:
2. Разработка комплекса мер:
3. Оценка эффективности
4. Планирование внедрения:
5. Анализ текущего состояния системы защиты

Запишите ответ:

1	
2	
3	
4	
5	

Ключи ответов

Номер задания	Правильный ответ	
	1 вариант	2 вариант
1	б	г
2	а	в
3	а	а
4	а, б, в	б
5	а	а
6	г	а
7	1-е,2-в. 3-а, 4- б, 5-д, 6-г	1-в. 2-д. 3-б. 4-г, 5-а, 6-д
8	5	1-б. 2-в, 3-а
9	а	а, б, в, г
10	1-4, 2-1, 3- 2, 4-3. 5-5	а, в, б, г
11	1-е, 2-в, 3-а, 4-б, 5-д, 6-г	а
12	в	1-в, 2-а, 3-б, 4-г, 5-е, 6-д
13	а	б
14	в	б
15	5,1,2,6,4,3	б
16	дестабилизирующие	в
17	в	1-д, 3-в, 2-г, 4-б, 5-а
18	г	г
19	5,1,4,3,2	г
20	д, г, в, б, а	а
21	г	1-в,2-в,3-а, 4-д, 5-г
22	г	б
23	а,б,в	дестабилизирующее
24	а	б
25	5,3,2.4,1	5, 1, 2, 4, 3

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-13 баллов	2 (неудовлетворительно)	0-50%	низкий
14-17 баллов	3 (удовлетворительно)	51-65%	базовый
18-21 баллов	4 (хорошо)	66-85%	повышенный
22-25 баллов	5 (отлично)	86-100%	высокий

Раздел 2. Защита автономных автоматизированных систем

Вариант 1

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
1. Какие основные угрозы информационной безопасности существуют для автономных автоматизированных систем? ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)***
а) Перехват данных, отказ в обслуживании, вредоносное ПО
б) Подмена данных, изменение конфигурации, физические повреждения
в) Угрозы социального инжиниринга, фишинга, утечки данных
г) Все вышеперечисленные

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
4. Что такое аутентификация в контексте защиты информации? ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2, З3, ПК. 2.4, ПК. 2.6)***
а) Процесс проверки подлинности пользователя или устройства
б) Процесс ограничения доступа к ресурсам
в) Процесс восстановления утраченных данных
г) Процесс обновления программного обеспечения

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое шифрование данных и зачем оно используется? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
а) Метод сжатия данных для экономии места
б) Метод преобразования данных в нечитаемый вид для предотвращения несанкционированного доступа
в) Метод дублирования данных для повышения надежности
г) Метод ускоренной передачи данных

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.
Что такое контроль целостности данных и почему он важен? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
а) Процесс верификации правильности и полноты данных после передачи или хранения
б) Процесс удаления устаревших данных
в) Процесс резервного копирования данных
г) Процесс верификации правильности и полноты данных после передачи или хранения

Задание №5. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое контроль целостности данных и почему он важен? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***

а) Процесс верификации правильности и полноты данных после передачи или хранения

б) Процесс удаления устаревших данных

в) Процесс резервного копирования данных

г) Процесс верификации правильности и полноты данных после передачи или хранения

Задание №6. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.

Необходимо разработать комплекс мер по защите автономных автоматизированных систем от кибератак и других видов деструктивного воздействия. Рассмотрите следующие аспекты и выверите для них соответствующие действия: ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)***

1. Классификация угроз	а) Проведите анализ типичных уязвимостей ААС. Предложите методы их устранения или минимизации.
2. Анализ уязвимостей	б) Определите основные категории угроз, которым подвержены ААС.
3. Разработка защитных мер	в) Опишите подходы к созданию многослойной защиты ААС. Укажите, какие программные и аппаратные средства могут быть использованы для повышения уровня безопасности.
4. Мониторинг и реагирование	г) Составьте программу обучения для инженеров и операторов ААС по вопросам информационной безопасности.
5. Обучение и подготовка персонала	д). Предложите систему мониторинга состояния безопасности ААС. Разработайте план действий в случае обнаружения угрозы или инцидента.

Запишите ответ:

1	
2	
3	
4	
5	

Задание №7. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Что понимается под защитой программ от изучения? ***(оцениваемые знания, умения, компетенции: У2, У5, З1, ПК. 2.2, ПК. 2.3)***
а) Меры, направленные на предотвращение легального использования программы
б) Меры, направленные на затруднение понимания и модификации исходного кода программы
в) Меры, предназначенные для улучшения производительности программы
г) Меры, обеспечивающие совместимость программы с разными операционными системами.

Задание №8. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Зачем применяется шифрование исполняемых файлов? ***(оцениваемые знания, умения, компетенции: У2, У5, З1, ПК. 2.2, ПК. 2.3)***
а) Для защиты данных, передаваемых программой
б) Для предотвращения несанкционированного доступа к содержимому исполняемого файла
в) Для ускорения загрузки программы
г) Для упрощения установки программы.

Задание №9. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие подходы применяются для защиты программ от обратного инжиниринга? ***(оцениваемые знания, умения, компетенции: У2, У5, З1, ПК. 2.2, ПК. 2.3)***
а) Анти-отладочные техники
б) Водяные знаки
в) Защита от дизассемблирования

Задание №10. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Что такое вредоносное программное обеспечение (malware)? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***
а) Программы, разработанные для облегчения работы пользователей
б) Программы, предназначенные для предоставления обновлений безопасности
в) Программы, созданные для нанесения вреда компьютеру или сети
г) Программы, используемые для оптимизации работы операционной системы

Задание №11. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.
Чем отличается вирус от червя? ***(оцениваемые знания, умения,***

компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)

а) Вирус требует действий пользователя для распространения, тогда как червь распространяется автоматически

б) Червь поражает только определенные файлы, а вирус — всю систему

в) Вирус удаляет данные, а червь их шифрует

г) Вирус требует действий пользователя для распространения, тогда как червь распространяется автоматически

Задание №12. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.

Как работает рекламное ПО (adware)? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

а) Показывает нежелательную рекламу на компьютере пользователя

б) Собирает личные данные пользователя и передает их третьим лицам

в) Открывает браузер на определенных сайтах

г) Показывает нежелательную рекламу на компьютере пользователя.

Задание №13. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.

Что такое защита программ и данных от несанкционированного копирования? ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Меры, направленные на облегчение копирования программ и данных

б) Меры, обеспечивающие совместимость программ с различными устройствами

в) Меры, препятствующие незаконному воспроизведению и распространению программ и данных

г) Меры, повышающие производительность программ

Задание №14. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.

1. **Что такое цифровая подпись и как она помогает защитить программы?** ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Подпись автора программы, добавленная в исходный код

б) Криптографический метод подтверждения подлинности и целостности программы

в) Водяной знак, добавляемый в графические файлы

г) Специальный файл, содержащий лицензию на использование программы

Задание №15. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.

2. **Какие меры защиты данных от несанкционированного копирования применяются?** ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Шифрование данных

б) Ограничение доступа к данным через права пользователей
в) Использование технологий цифровой подписи для подтверждения целостности данных

Задание №16. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.
1. **Что такое машинные носители информации?** ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***
а) Бумажные документы, содержащие информацию
б) Электронные устройства, хранящие информацию (жесткие диски, флеш-накопители и др.)
в) Серверы и облачные хранилища
г) Электронные устройства, хранящие информацию (жесткие диски, флеш-накопители и др.)

Задание №17. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.
Какие методы защиты информации на машинных носителях применяются? ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***
а) Шифрование данных
б) Контроль доступа и аутентификация
в) Резервное копирование
г) Все вышеперечисленные

Задание №18. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.
Что такое резервное копирование и зачем оно нужно? ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***
а) Процедура создания копии данных для последующего восстановления в случае их потери или повреждения
б) Процедура шифрования данных для предотвращения несанкционированного доступа
в) Процедура удаления ненужных данных
г) Процедура создания копии данных для последующего восстановления в случае их потери или повреждения

Задание №19. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.
Какие юридические меры могут быть применены для защиты информации на машинных носителях? ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***

а) Законы о защите персональных данных
б) Договоры о неразглашении информации
в) Политики компании по использованию ИТ-ресурсов

Задание №20. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.

Необходимо разработать процесс внедрения программного продукта от изучения и модификации, необходимо выполнить установку по этапам, последовательно. ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***:

- **Этап 1**: Выбор и приобретение необходимых инструментов.
- **Этап 2**: Обучение сотрудников использованию новых инструментов.
- **Этап 3**: Интеграция инструментов в существующую инфраструктуру.
- **Этап 4**: Анализ требований и выбор методов защиты.
- **Этап 5**: Постоянный мониторинг и аудит соблюдения политики.
- Запишите ответ:

1	
2	
3	
4	
5	

Задание №21. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.

Что такое аппаратные средства идентификации и аутентификации? (оцениваемые знания, умения, компетенции: У3, У5, У4, З3, З5, ПК. 2.6, ПК. 2.3, ПК.2.2)

а) Программные приложения, проверяющие личность пользователя
б) Устройства, подтверждающие личность пользователя с помощью биометрии
в) Физические устройства, используемые для подтверждения личности пользователя и предоставления доступа к системе
г) Компоненты компьютерной системы, отвечающие за хранение данных

Задание №22. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов.

Что такое смарт-карта и как она используется для аутентификации? (оцениваемые знания, умения, компетенции: У3, У5, У4, З3, З5, ПК. 2.6, ПК. 2.3, ПК.2.2)

а) Карта с магнитной полосой, используемая для хранения финансовых данных
б) Микропроцессорная карта, содержащая уникальный идентификатор и/или

сертификат, который используется для подтверждения личности пользователя
в) Карта с чипом, применяемая для оплаты проезда в общественном транспорте
г) Карта с QR-кодом, используемая для входа в здания

Задание №23. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.
Какие недостатки есть у биометрической аутентификации? (оцениваемые знания, умения, компетенции: У3, У5, У4, З3, З5, ПК. 2.6, ПК. 2.3, ПК.2.2)
а**)** Высокие затраты на внедрение и обслуживание
б) Возможные ошибки при распознавании
в) Проблемы с конфиденциальностью данных

Задание №24. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.
1. **Какие преимущества имеет гибридная система обнаружения атак?** ***(оцениваемые знания, умения, компетенции: У3, У2, У10, З3, З2, ПК. 2.6, ПК. 2.3)***
а) Более точное обнаружение атак благодаря сочетанию методов
б) Уменьшенное количество ложных срабатываний
в) Возможность адаптации к новым видам угроз
г) Все вышеперечисленные

Задание №25. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.
Какие компоненты обычно включают в себя системы обнаружения атак и вторжений? ***(оцениваемые знания, умения, компетенции: У3, У2, У10, З3, З2, ПК. 2.6, ПК. 2.3)***
а) Сенсоры для сбора данных
б) Модули анализа и корреляции данных
в) Консоль управления и оповещения

Вариант 2

Задание №1. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие меры применяются для защиты автономных автоматизированных систем от несанкционированного доступа? ***(оцениваемые знания, умения, компетенции: У3, У5, , З1, З2,З3, ПК. 2.4, ПК. 2.6)***
а) Аутентификация и авторизация пользователей
б) Контроль доступа и мониторинг активности
в) Шифрование данных и каналов связи
г) Все вышеперечисленные.

Задание №2. Выберите правильные варианты ответов и обведите

кружочками буквы правильных ответов
Какие способы аутентификации наиболее часто используются в автономных системах? ***(оцениваемые знания, умения, компетенции: У3, У5, , 31, 32,33, ПК. 2.4, ПК. 2.6)***
а) Пароли и PIN-код
б) Биометрическая идентификация (отпечатки пальцев, распознавание лица)
в) Смарт-карты и токены

Задание №3. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие меры предпринимаются для защиты автономных систем от физического вмешательства? ***(оцениваемые знания, умения, компетенции: У3, У5, , 31, 32,33, ПК. 2.4, ПК. 2.6)***
а) Ограниченный физический доступ к оборудованию
б) Использование датчиков вторжения и сигнализации
в) Скрытие и маскировка ключевых компонентов системы

Задание №4. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие подходы используются для мониторинга и анализа безопасности автономных систем? ***(оцениваемые знания, умения, компетенции: У3, У5, , 31, 32,33, ПК. 2.4, ПК. 2.6)***
)а) Логирование событий и анализ журналов
б) Мониторинг сетевого трафика и аномалий
в) Использование систем обнаружения вторжений (IDS/IPS)
г) Все вышеперечисленные.

Задание №5. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие методы используются для защиты программ от изучения?
(оцениваемые знания, умения, компетенции: У2, У5, , 31, ПК. 2.2, ПК. 2.3)
а) Обфускация кода
б) Шифрование исполняемых файлов
в) Использование виртуальных машин
г) Все вышеперечисленные

Задание №6. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие риски связаны с использованием виртуальных машин для защиты программ? ***(оцениваемые знания, умения, компетенции: У2, У5, , 31, ПК. 2.2, ПК. 2.3)***
а) Высокая нагрузка на ресурсы компьютера
б) Возможность обхода защиты через эмуляторы
в) Ограниченные возможности взаимодействия с операционной системой

г) Установка программ на ПК

Задание №7. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Какие правовые механизмы могут применяться для защиты программ от нелегального использования? ***(оцениваемые знания, умения, компетенции: У2, У5, З1, ПК. 2.2, ПК. 2.3)***

а) Лицензионные соглашения
б) Авторское право
в) Патенты
г) Все вышеперечисленные.

Задание №8. Прочитайте ситуационную задачу и установите последовательность. В таблицу запишите правильную последовательность.

Необходимо разработать процесс внедрения программного продукта от изучения и модификации, необходимо выполнить установку по этапам, последовательно.
(оцениваемые знания, умения, компетенции: У2, У5, З1, ПК. 2.2, ПК. 2.3)

- **Этап 1**: Внедрение системы мониторинга и анализа эффективности защиты.
- **Этап 2**: Тестирование и отладка защищенного кода
- **Этап 3**: Интеграция выбранных инструментов в процесс сборки и деплоя.
- **Этап 4**: Анализ требований и выбор методов защиты

Запишите ответ:

1	
2	
3	
4	

Задание №9. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов

Какие основные типы вредоносного программного обеспечения существуют? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

а) Все шеперечисленные
б) Рекламное ПО, шпионское ПО, руткиты
в) Ботнеты, кейлоггеры, эксплойты
г) Вирусы, черви, трояны

Задание №10. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Что делает троянская программа? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***

а) Распространяется через электронную почту и заражает компьютер вирусом
б) Создает ботнет для проведения DDoS-атак

в) Маскируется под полезную программу, но на самом деле выполняет вредоносные действия
г) Шифрует данные и требует выкуп за их расшифровку.

Задание №11. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что делает шпионское ПО (spyware)? ***(оцениваемые знания, умения, компетенции: У3, У4, У10, З1, З2, З6, ПК. 2.2, ПК. 2.3)***
а) Пытается получить доступ к личным данным пользователя без его ведома
б) Использует ресурсы компьютера для майнинга криптовалют
в) Изменяет настройки браузера
г) Пытается получить доступ к личным данным пользователя без его ведома.

Задание №12. Прочитайте ситуационную задачу и установите соответствия между аспектами и действиями. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Ответ запишите в таблицу.
Необходимо разработать план действий по устранению последствий заражения и предотвратить подобные инциденты в будущем. Рассмотрите следующие аспекты:
Необходимо разработать комплекс мер по защите автономных автоматизированных систем от кибератак и других видов деструктивного воздействия. Рассмотрите следующие аспекты и выверите для них соответствующие действия: ***(оцениваемые знания, умения, компетенции: У3, У5, З1, З2,З3, ПК. 2.4, ПК. 2.6)***

1. Диагностика и устранение инфекции	а) Предложите инструменты и методики для очистки системы и перечислите шаги для диагностики и удаления ВПО с сервера?
2.Восстановление данных	б) Организовать обучение сотрудников для повышения их осведомленности о ВПО и способах его распространения.
3.Профилактика будущих инфекций	в) Предложите меры для предотвращения повторного заражения ВПО, технологии и политики безопасности для защиты системы систему мониторинга состояния безопасности ААС.
4.Обучение и информирование сотрудников	г) Предложите варианты восстановления данных для минимизировать потери данных и восстановления работоспособности системы?

Запишите ответ:

1	
2	
3	

4	

Задание №13. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов

Какие методы защиты программ от несанкционированного копирования существуют? ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Все шеперечисленные
б) Активации программного продукта через интернет
в) Интеграция ключей защиты (dongles)
г) Использование цифровых подписей

Задание №14. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов

Какие способы активации программного продукта используются для защиты от копирования? ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Онлайн-активация через официальный сайт производителя
б) Активация с помощью серийного номера
в) Использование уникальных аппаратных идентификаторов (например, MAC-адрес)

Задание №15. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Какие юридические меры могут быть использованы для защиты программ и данных от копирования? ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Все вышеперечисленные
б) Патенты
в) Лицензии и договоры
г) Авторские права

Задание №16. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие юридические меры могут быть использованы для защиты программ и данных от копирования? ***(оцениваемые знания, умения, компетенции: У1, У5, У4, З1, З3, З5, ПК. 2.2, ПК. 2.3, ПК. 2.4)***

а) Авторские права
б) Патенты
в) Лицензии и договоры

Задание №17. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.

2. **Какие основные угрозы для информации на машинных носителях существуют?** ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***

а) Потеря или повреждение носителя
б) Несанкционированный доступ к данным
в) Вирусные атаки и вредоносное ПО
г) Работа с информацией

Задание №18. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.

3. **Какие методы контроля доступа к информации на машинных носителях применяются?** ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***

а) Парольные защиты
б) Биометрическая аутентификация
в) Многофакторная аутентификация
г) Имя носителя

Задание №19. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов.

Какие меры предосторожности следует соблюдать при работе с мобильными носителями информации (флеш-накопители, внешние жесткие диски)? ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***

а) Использование антивирусного ПО
б) Шифрование данных на носителе
в) Ограничение доступа к носителю
г) Работа в режиме

Задание №20. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов.

4. **Какие организационные меры помогают обеспечить защиту информации на машинных носителях?** ***(оцениваемые знания, умения, компетенции: У2, У10, У4, З1, З2, З5, З6, ПК. 2.5, ПК. 2.3, ПК. 2.4, ПК.2.2)***

а) Все вышеперечисленные
б) Регулярные аудиты безопасности
в) Установление политик и процедур безопасного обращения с информацией
г) Обучение сотрудников основам кибербезопасности

Задание №21. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Какие типы аппаратных средств идентификации и аутентификации существуют? ***(оцениваемые знания, умения, компетенции: У3, У5, У4, З3, З5, ПК. 2.6, ПК. 2.3, ПК.2.2)***

а) Смарт-карты, USB-токены, RFID-метки

б) Все вышеперечисленные
в) Сканеры штрих-кодов, считыватели магнитных карт
г) Биометрические сканеры (отпечатков пальцев, радужки глаза)

Задание №22. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие биометрические характеристики чаще всего используются для аутентификации? *(оцениваемые знания, умения, компетенции: У3, У5, У4, З3, З5, ПК. 2.6, ПК. 2.3, ПК.2.2)*
а) Отпечатки пальцев, радужка глаза, форма лица
б) Голос, походка, ДНК
в) Рисунок вен, геометрия руки, подпись
г) Отпечатки пальцев, радужка глаза, форма лица

Задание №23. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие основные типы систем обнаружения атак и вторжений существуют? (оцениваемые знания, умения, компетенции: У3, У2, У10, З3, З2, ПК. 2.6, ПК. 2.3)
а)Системы на основе сигнатур (signature-baseг)
б) Системы на основе аномалий (anomaly-baseг)
в) Гибридные системы
г) Все вышеперечисленные.

Задание №24. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие компоненты обычно включают в себя системы обнаружения атак и вторжений? *(оцениваемые знания, умения, компетенции: У3, У2, У10, З3, З2, ПК. 2.6, ПК. 2.3)*
а) Все вышеперечисленные
б) Модули анализа и корреляции данных
в) Консоль управления и оповещения
г) Сенсоры для сбора данных

Задание №25. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие основные типы систем обнаружения атак и вторжений существуют? *(оцениваемые знания, умения, компетенции: У3, У2, У10, З3, З2, ПК. 2.6, ПК. 2.3)*
а) Системы на основе сигнатур (signature-baseг)
б) Системы на основе аномалий (anomaly-baseг)
в) Гибридные системы

Ключи ответов

Номер	Правильный ответ

задания	1 вариант	2 вариант
1	г	г
2	б	а, б, в
3	б	а, б, в
4	г	г
5	г	г
6	1-б, 2-а, 3-в, 4- д, 5- г	а, б, в
7	б	г
8	б	4, 3, 2, 1
9	а,б,в,г	а
10	в	в
11	г	г
12	г	1-а, 2-г, 3-в, 4-б
13	в	а
14	б	а, б, в
15	а, б, в	а
16	г	а, б, в
17	г	а, б, в
18	г	а, б, в
19	а, б, в	а, б, в
20	4, 1, 3, 2, 5	а
21	в	а, б, г
22	в	а
23	а, б, в	г
24	г	а
25	а, б, в	а, б, в

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-13аллов	2 (неудовлетворительно)	0-50%	низкий
14-17 баллов	3 (удовлетворительно)	51-65%	базовый
18-21 баллов	4 (хорошо)	66-85%	повышенный
22-25 баллов	5 (отлично)	86-100%	высокий

Раздел 3. Защита информации в локальных сетях
1 вариант

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

1. **Что такое защищённая сеть?** ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)*** **доступа и обеспечить безопасность**

а) Сеть, в которой используется только проводное соединение

б) Сеть, которая обеспечивает высокий уровень производительности

в) **Сеть, спроектированная и настроенная таким образом, чтобы минимизировать риск несанкционированного доступа к передаваемой информации**

г) Сеть, доступная только определённым пользователям

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какова основная функция межсетевого экрана (firewall)? ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

а) Контролирует доступ к веб-сайтам

б)Фильтрует входящий и исходящий сетевой трафик на основе заранее установленных правил

в) Обеспечивает шифрование данных

г) Блокирует вирусы

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие типы систем обнаружения вторжений существуют? ***(оцениваемые знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)***

а) Системы на основе сигнатур

б) Системы на основе аномалий

в) Гибридные системы

Задание №4. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Что такое OpenVPN? ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

а) Открытый стандарт для маршрутизации пакетов в Интернете

б) Открытое программное обеспечение для создания VPN с открытым исходным кодом

в) Бесплатный сервис для обмена файлами

г) Система для мониторинга сетевого трафика

Задание №5. Прочитайте текст и впишите пропущенное слово в предложение. ***(оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).***

….. – это открытое программное обеспечение для создания VPN с открытым исходным кодом
Запишите ответ:

Задание №6. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какова основная функция межсетевого экрана (firewall)? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Контролирует доступ к веб-сайтам
б) Фильтрует входящий и исходящий сетевой трафик на основе заранее установленных правил
в) Обеспечивает шифрование данных
г) Блокирует вирусы

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие меры защиты могут быть приняты для защиты беспроводных сетей? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Использование WPA2/WPA3-шифрования
б) Фильтрация MAC-адресов
в) Скрытие SSID

Задание №8. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие устройства могут использоваться для организации VPN?
(оцениваемые знания, умения, компетенции: У3, У1, 31, 33, ПК. 2.2, ПК. 2.1).
а) Маршрутизаторы, межсетевые экраны (firewalls), специализированные VPN-устройства
б) Серверы, рабочие станции, мобильные устройства
в) Принт-серверы, файловые серверы, почтовые серверы

Задание №9. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие основные элементы включаются в архитектуру защищённой сети? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Маршрутизаторы, коммутаторы, сервера
б) Межсетевые экраны (firewall), системы обнаружения вторжений (IDS), виртуальные частные сети (VPN)
в) Системы управления доступом (ACS), антивирусное ПО, системы мониторинга трафика

Задание №10. Выберите правильный вариант ответов и обведите

кружочками буквы правильных ответов

Что такое виртуальная частная сеть (VPN)? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***

а) Частная сеть, доступная только сотрудникам компании

б) Технология, создающая зашифрованное соединение через общедоступные сети, обеспечивая безопасный обмен данными

в) Локальная сеть, соединяющая несколько офисов

г) Технология, используемая для обмена мгновенными сообщениями

Вариент2

Задание №1. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Какие основные элементы включаются в архитектуру защищённой сети? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***

а) Маршрутизаторы, коммутаторы, сервера

б) Межсетевые экраны (firewall), системы обнаружения вторжений (IDS), виртуальные частные сети (VPN)

в) Системы управления доступом (ACS), антивирусное ПО, системы мониторинга трафика

г) Все вышеперечисленные

Задание №2. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Что такое виртуальная частная сеть (VPN)? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***

а) Частная сеть, доступная только сотрудникам компании

б) Технология, создающая зашифрованное соединение через общедоступные сети, обеспечивая безопасный обмен данными

в) Локальная сеть, соединяющая несколько офисов

г) Технология, используемая для обмена мгновенными сообщениями

Задание №3. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов

Каковы основные функции системы обнаружения вторжений (IDS)? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***

а) Блокирует подозрительный трафик

б) Обнаруживает попытки несанкционированного доступа и предупреждает администратора

в) Управляет правами доступа пользователей

г) Защищает от вирусов

Задание № 4. Прочитайте текст и впишите пропущенное слово в предложение. ***(оцениваемые знания, умения, компетенции: У3, У1, 31, 33, ПК. 2.2, ПК. 2.1).***

….. – это т**ехнология, позволяющая создавать защищённые каналы связи**

через небезопасные сети, такие как Интернет
Запишите ответ:

Задание №5. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Что такое защищённая сеть? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Сеть, в которой используется только проводное соединение
б) Сеть, которая обеспечивает высокий уровень производительности
в) Сеть, спроектированная и настроенная таким образом, чтобы минимизировать риск несанкционированного сность передаваемой информации
г) Сеть, доступная только определённым пользователям

Задание №6. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какова основная функция межсетевого экрана (firewall)? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Контролирует доступ к веб-сайтам
б) Фильтрует входящий и исходящий сетевой трафик на основе заранее установленных правил
в) Обеспечивает шифрование данных
г) Блокирует вирусы

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие типы систем обнаружения вторжений существуют? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)***
а) Системы на основе сигнатур
б) Системы на основе аномалий
в) Гибридные системы

Задание №8. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Что такое защищённая сеть? ***(оцениваемые знания, умения, компетенции: У3, 31, 36, ПК. 2.2, ПК. 2.4)*** **доступа и обеспечить безопа**
а) Сеть, в которой используется только проводное соединение
б) Сеть, которая обеспечивает высокий уровень производительности
в) Сеть, спроектированная и настроенная таким образом, чтобы минимизировать риск несанкционированного сность передаваемой информации
г) Сеть, доступная только определённым пользователям

Задание №9. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какова основная функция межсетевого экрана (firewall)? ***(оцениваемые***

знания, умения, компетенции: У3, З1, З6, ПК. 2.2, ПК. 2.4)
а) Контролирует доступ к веб-сайтам
б) Фильтрует входящий и исходящий сетевой трафик на основе заранее установленных правил
в) Обеспечивает шифрование данных
г) Блокирует вирусы

Задание №10. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие устройства могут использоваться для организации VPN? (оцениваемые знания, умения, компетенции: У3, У1, З1, З3, ПК. 2.2, ПК. 2.1).
а) Маршрутизаторы, межсетевые экраны (firewalls), специализированные VPN-устройства
б) Серверы, рабочие станции, мобильные устройства
в) Принт-серверы, файловые серверы, почтовые серверы

Ключи ответов

Номер задания	Правильный ответ	
	1 вариант	2 вариант
1	в	г
2	б	б
3	а,б,в	б
4	б	OpenVPN
5	OpenVPN	в
6	б	б
7	а,б,в	а,б,в
8	а	в
9	б	б
10	б	а

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-5 баллов	2 (неудовлетворительно)	0-50%	низкий
6-7 баллов	3 (удовлетворительно)	50-70%	базовый

8-9 баллов	4 (хорошо)	80-90%	повышенный
10 баллов	5 (отлично)	100%	высокий

Раздел 4. Защита информации в сетях общего доступа

Вариерт1

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что такое межсетевое взаимодействие? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Передача данных между различными сетями
б) Совместная работа нескольких компьютерных сетей для обмена данными
в) Объединение пользователей в социальные сети
г) Создание локальной сети внутри одной организации

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие меры безопасности применяются для защиты межсетевого взаимодействия? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Использование межсетевых экранов (firewalls)
б) Шифрование данных
в) Системы обнаружения вторжений (IDS)
г) Все вышеперечисленные

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие типы межсетевых экранов существуют? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Пакетные фильтры
б) Прокси-серверы
в) Stateful firewalls
г) Все вышеперечисленные

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие преимущества предоставляет использование VPN? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Повышенная безопасность передачи данных
б) Сокрытие реального IP-адреса
в) Возможность удалённого доступа к внутренним ресурсам
г) Все вышеперечисленные

Задание №5. Прочитайте ситуационную задачу и определите необходимые шаги для ее решения. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6)
***Задача*:** Компания "Пример ЛТД" планирует развернуть корпоративную сеть, объединяющую несколько офисов, расположенных в разных городах. В сети будут передаваться конфиденциальные данные клиентов, финансовые отчеты и другая важная информация. Необходимо обеспечить безопасность межсетевого взаимодействия между офисами компании, чтобы предотвратить утечки данных и несанкционированный доступ.
Требования:

1. Защита передаваемых данных от перехвата (конфиденциальность).
2. Аутентификация пользователей и устройств, участвующих в обмене данными.
3. Предотвращение атак типа "человек посередине" (MITM).
4. Защита от DoS-атак
5. Контроль доступа и мониторинг сетевой активности.
6. Соответствие нормативным требованиям и стандартам информационной безопасности

1	
2	
3	
4	
5	
6	

Вариани 2

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие основные угрозы существуют при межсетевом взаимодействии? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Атаки типа "отказ в обслуживании" (DDoS)
б) Перехват данных (man-in-the-middle attack)
в) Вторжение в сеть (intrusion)
г) Все вышеперечисленные

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Что такое межсетевой экран (firewall)? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Устройство для разгрузки сети
б) Устройство или программное обеспечение, контролирующее входящий и исходящий сетевой трафик на основе заданных правил

в) Программа для шифрования данных
г) Система для мониторинга трафика

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие преимущества предоставляет использование VPN? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Повышенная безопасность передачи данных
б) Сокрытие реального IP-адреса
в) Возможность удалённого доступа к внутренним ресурсам
г) Все вышеперечисленные

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие меры безопасности рекомендуется применять для защиты межсетевого взаимодействия? ***(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Регулярное обновление программного обеспечения
б) Настройка строгих правил межсетевого экрана
в) Использование шифрования данных
г) Все вышеперечисленные

Задание №5. Прочитайте ситуационную задачу и определите необходимые шаги для ее решения. Ответ запишите в таблицу.
(оцениваемые знания, умения, компетенции: У2, У9, У10, З1, З3, ПК. 2.2, ПК. 2.3, ПК2.6)
***Задача*:** Компания "Пример ЛТД" планирует развернуть корпоративную сеть, объединяющую несколько офисов, расположенных в разных городах. В сети будут передаваться конфиденциальные данные клиентов, финансовые отчеты и другая важная информация. Необходимо обеспечить безопасность межсетевого взаимодействия между офисами компании, чтобы предотвратить утечки данных и несанкционированный доступ.
Требования:

1. Защита передаваемых данных от перехвата (конфиденциальность).
2. Аутентификация пользователей и устройств, участвующих в обмене данными.
3. Предотвращение атак типа "человек посередине" (MITM).
4. Защита от DoS-атак.
5. Контроль доступа и мониторинг сетевой активности.
6. Соответствие нормативным требованиям и стандартам информационной безопасности

1	
2	
3	
4	

5	
6	

Ключи ответов

Номер задания	Правильный ответ	
	1 вариант	2 вариант
1	б	г
2	г	б
3	г	г
4	г	г
5	1. Использование VPN 2. Фильтрация и контроль трафика 3. Аутентификация и управление доступом 4. Мониторинг и аудит 5. Резервирование и восстановление 6. Обучение персонала	1. Использование VPN 2. Фильтрация и контроль трафика 3. Аутентификация и управление доступом 4. Мониторинг и аудит 5. Резервирование и восстановление 6. Обучение персонала

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-2 баллов	2 (неудовлетворительно)	0-50%	низкий
3 баллов	3 (удовлетворительно)	60%	базовый
4 баллов	4 (хорошо)	80%	повышенный
5 баллов	5 (отлично)	100%	высокий

Раздел 5. Защита информации в базах данных
1 вариант

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое база данных? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Набор таблиц, содержащих структурированную информацию

б) Программное обеспечение для обработки запросов
в) Система управления файлами
г) Набор таблиц, содержащих структурированную информацию

Задание №2. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие методы аутентификации пользователей в базах данных используются? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Простая аутентификация с использованием имени пользователя и пароля
б) Двухфакторная аутентификация
в) Аутентификация на основе сертификатов

Задание №3. Выберите правильный вариант ответов и обведите кружочками буквы правильных ответов
Какие методы шифрования данных в базах данных применяются? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Симметричное шифрование (AES, DES)
б) Асимметричное шифрование (RSA, ECB)
в) Хэширование (MD5, SHA-256)
г) Все вышеперечисленные

Задание №4. Выберите правильные варианты ответов и обведите кружочками буквы правильных ответов
Какие роли могут быть назначены пользователям в базах данных? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Администратор
б) Пользователь с ограниченными правами
в) Гость

Задание №5. Прочитайте ситуационную задачу и наудите соответствие с левого столбцы и информация с правого столбца. Ответы запишите в таблицу.
Необходимо разработать план мероприятий по защите информации в базах данных вашей компании, чтобы минимизировать риск повторных атак и защитить данные от утечек. ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***
Требования:

1.Конфиденциальность данных	а) Убедитесь, что данные не могут быть изменены или удалены без разрешения
2.Целостность данных	б) Обеспечьте доступность данных для авторизованных пользователей даже в условиях атак..

3.Доступность данных	в) Защитите данные от несанкционированного доступа
4.Соответствие нормативным требованиям	г) Разработайте решение, соответствующее международным стандартам безопасности данных (например, GDPR, PCI DSS).

Запишите ответ:

1	
2	
3	
4	

2 вариант

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие основные угрозы безопасности информации в базах данных существуют? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) отсутствие запросов на ПК
б) плохо оформлена таблица
в) Ненадёжные пароли

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое шифрование данных в базах данных? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Процесс перевода данных в читаемый формат
б) Процесс преобразования данных в нечитаемый вид для предотвращения несанкционированного доступа
в) Метод ускорения поиска данных
г) Способ удаления данных

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое контроль доступа в базах данных? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Ограничение прав пользователей на выполнение определённых операций с данными
б) Процесс аутентификации пользователей
в) Создание резервных копий данных
г) Ограничение прав пользователей на выполнение определённых операций с данными

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие меры безопасности рекомендуется применять для защиты

информации в базах данных? ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Регулярное обновление программного обеспечения

б) Регулярное создание резервных копий

в) Мониторинг активности пользователей

Задание №5. Прочитайте ситуационную задачу и наудите соответствие с левого столбцы и информация с правого столбца. Ответы запишите в таблицу.

Необходимо разработать план мероприятий по защите информации в базах данных вашей компании, чтобы минимизировать риск повторных атак и защитить данные от утечек. ***(оцениваемые знания, умения, компетенции: У3, У4, У5, З1, З4, ПК. 2.2, ПК. 2.3, ПК2.6).***

Требования:

1.Конфиденциальность данных	а) Разработайте решение, соответствующее международным стандартам безопасности данных (например, GDPR, PCI DSS).
2.Целостность данных	б) Обеспечьте доступность данных для авторизованных пользователей даже в условиях атак.
3.Доступность данных	в) Защитите данные от несанкционированного доступа
4.Соответствие нормативным требованиям	г) Убедитесь, что данные не могут быть изменены или удалены без разрешения

Запишите ответ:

1	
2	
3	
4	

Ключи ответов

Номер задания	Правильный ответ	
	1 вариант	2 вариант
1	г	в
2	а,б,в	б
3	г	г
4	а,б,в	а,б,в
5	1в 2а 3б 4г	1. в 2. г 3. б 4. а

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-2 баллов	2 (неудовлетворительно)	0-50%	низкий
3 баллов	3 (удовлетворительно)	60%	базовый
4 баллов	4 (хорошо)	80%	повышенный
5 баллов	5 (отлично)	100%	высокий

Раздел 6. Мониторинг систем защиты

Вариант 1

Задание №1. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое мониторинг систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6)***

а) Постоянное наблюдение за состоянием информационной безопасности

б) Регулярное обновление программного обеспечения

в) Процесс шифрования данных

г) Постоянное наблюдение за состоянием информационной безопасности

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие методы мониторинга систем защиты используются? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Анализ журналов событий

б) Использование систем обнаружения вторжений (IDS)

в) Мониторинг сетевого трафика

г) Все вышеперечисленные

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответовКакие основные задачи решает мониторинг систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Выявление потенциальных угроз

б) Оценка эффективности существующих мер безопасности

в) Определение источников атак

Задание №4. Выберите правильные вариант ответов и обведите

кружочками буквы правильных ответов

Какие меры безопасности рекомендуется применять для эффективного мониторинга систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Регулярное обновление программного обеспечения

б) Настройка строгих правил межсетевого экрана

в) Использование шифрования данных

Задание №5. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие критерии важны при выборе программно-аппаратного комплекса? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Производительность

б) Совместимость с существующими системами

в) Стоимость владения и обслуживания

г) Все вышеперечисленные

Задание №6. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое системы обнаружения вторжений (IDS)? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Программное обеспечение для удаления вирусов

б) Системы, предназначенные для обнаружения попыток несанкционированного доступа и вторжения в сеть

в) Системы для шифрования данных

г) Системы для резервного копирования данных

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие области применения программно-аппаратных комплексов являются наиболее популярными? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Телекоммуникации

б) Безопасность и видеонаблюдение

в) Медицина и биотехнологии

г) Все вышеперечисленные

Задание №8. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое контроль доступа? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Ограничение прав пользователей на выполнение определённых операций с данными

б) Процесс аутентификации пользователей

в) Создание резервных копий данных

г) Ограничение прав пользователей на выполнение определённых операций с данными

Задание №9. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое шифрование данных? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Процесс перевода данных в читаемый формат

б) Процесс преобразования данных в нечитаемый вид для предотвращения несанкционированного доступа

в) Метод ускорения поиска данных

г) Способ удаления данных

Задание №10. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие основные угрозы информационной безопасности существуют? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Несанкционированный доступ к данным

б) Вирусные атаки

в) Атаки типа "отказ в обслуживании" (DDoS)

г) Все вышеперечисленные

Задание №11. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Вы получили уведомление о том, что один из ваших серверов был взломан. Каковы будут ваши первые шаги? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Немедленно восстановите сервер из резервной копии

б) Определите причину взлома и устраните уязвимость

в) Сообщите руководству о взломе

г) Определите причину взлома, устраните уязвимость, восстановите сервер и сообщите руководству

Задание №12. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Один из серверов вашей компании подвергся атаке, и часть данных была украдена. Какие действия вы предпримете сразу после инцидента? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Проведете анализ уязвимостей и закроете найденные дыры

б) Восстановите данные из резервных копий

в) Уведомите пострадавших пользователей и начнете расследование

г) Проведете анализ уязвимостей, закроете найденные дыры, восстановите данные из резервных копий и уведомите пострадавших пользователей

Задание №13. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Ваша организация использует межсетевой экран (firewall) для защиты своей сети. Недавно вы обнаружили, что некоторые сотрудники жалуются на медленную работу сети. Каковы ваши следующие шаги? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Увеличьте полосу пропускания интернет-канала

б) Отключите межсетевой экран, чтобы улучшить производительность

в) Проанализируйте правила межсетевого экрана и настройте их для оптимизации работы сети

г) Установите дополнительный межсетевой экран

Задание №14. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие преимущества предоставляют современные программно-аппаратные комплексы? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Повышенная производительность

б) Удобство в управлении и обслуживании

в) Интеграция с другими системами

г) Все вышеперечисленные

Задание №15. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие факторы влияют на эффективность работы программно-аппаратного комплекса? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Качество программного обеспечения

б) Надёжность аппаратных устройств

в) Уровень квалификации обслуживающего персонала

Задание №16. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие современные технологии используются в программно-аппаратных комплексах? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Искусственный интеллект и машинное обучение

б) Большие данные и аналитика

в) Интернет вещей (IoT)

г) Все вышеперечисленные

Задание №17. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Ваша компания использует распределённую вычислительную сеть, состоящую из множества узлов. Как вы планируете обеспечивать надёжность и отказоустойчивость такой системы? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

а) Внедрите избыточные узлы и компоненты

б) Используйте системы мониторинга и раннего предупреждения сбоев

в) Разработайте планы аварийного восстановления

г) Внедрите избыточные узлы и компоненты, используйте системы мониторинга и раннего предупреждения сбоев, разработайте планы аварийного восстановления

Задание №18. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Вы обнаружили, что одна из систем вашего комплекса подвержена атакам типа "отказ в обслуживании" (DDoS). Как вы будете реагировать на эту ситуацию? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

а) Установите межсетевой экран (firewall)

б) Настроите фильтрацию трафика

в) Обратитесь к поставщику услуг Интернета для блокировки подозрительного трафика

г) Настроите фильтрацию трафика, установите межсетевой экран и обратитесь к поставщику услуг Интернета для блокировки подозрительного трафика

Задание №19. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие современные технологии используются в программно-аппаратных комплексах? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Искусственный интеллект и машинное обучение

б) Большие данные и аналитика

в) Интернет вещей (IoT)

Задание №20. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие инновации внедряются в современные программно-аппаратные комплексы? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Облачные технологии

б) Виртуализация

в) Автономные системы

Вариант 2

Задание №1. Выберите правильные вариант ответов и обведите

кружочками буквы правильных ответов

Какие основные задачи решает мониторинг систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Выявление потенциальных угроз

б) Оценка эффективности существующих мер безопасности

в) Определение источников атак

г) Все вышеперечисленные

Задание №2. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое мониторинг сетевого трафика? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Процесс наблюдения за производительностью сети

б) Процесс анализа сетевого трафика для выявления подозрительных действий

в) Процесс обновления сетевого оборудования

г) Процесс управления доступом к сети

Задание №3. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое мониторинг систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Постоянное наблюдение за состоянием информационной безопасности

б) Регулярное обновление программного обеспечения

в) Процесс шифрования данных

г) Постоянное наблюдение за состоянием информационной безопасности

Задание №4. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Что такое мониторинг сетевого трафика? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Процесс наблюдения за производительностью сети

б) Процесс анализа сетевого трафика для выявления подозрительных действий

в) Процесс обновления сетевого оборудования

г) Процесс управления доступом к сети

Задание №5. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие меры безопасности рекомендуется применять для эффективного мониторинга систем защиты? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***

а) Регулярное обновление программного обеспечения

б) Настройка строгих правил межсетевого экрана

в) Использование шифрования данных

г) Все вышеперечисленные

Задание №6. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
. Какие современные технологии используются в программно-аппаратных комплексах? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
а) Искусственный интеллект и машинное обучение
б) Большие данные и аналитика
в) Интернет вещей (IoT)
г) Все вышеперечисленные

Задание №7. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие факторы влияют на эффективность работы программно-аппаратного комплекса? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
а) Качество программного обеспечения
б) Надёжность аппаратных устройств
в) Уровень квалификации обслуживающего персонала
г) Все вышеперечисленные

Задание №8. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие типы контроля доступа существуют? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Дискреционный контроль доступа (DAB)
б) Мандатный контроль доступа (MAB)
в) Ролевый контроль доступа (RBAB)

Задание №9. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие методы шифрования данных используются? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Симметричное шифрование (AES, DES)
б) Асимметричное шифрование (RSA, ECB)
в) Хэширование (MD5, SHA-256)

Задание №10. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие меры защиты информации в информационных системах применяются? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Шифрование данных

б) Контроль доступа
в) Системы обнаружения вторжений (IDS)
г) Все вышеперечисленные

Задание №11. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
10. В ходе мониторинга вы обнаружили, что кто-то пытается установить удалённый доступ к одному из ваших серверов. Как вы отреагируете? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6)***
.а) Блокируете попытку удалённого доступа и продолжаете мониторинг
б) Устанавливаете дополнительные меры безопасности на сервере
в) Оповещаете службу безопасности и расследуете инцидент
г) Блокируете попытку удалённого доступа, устанавливаете дополнительные меры безопасности, оповещаете службу безопасности и расследуете инцидент

Задание №12. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Сотрудники вашей компании сообщают, что стали получать подозрительные письма с вложениями. Вы подозреваете фишинговую атаку. Как вы справитесь с ситуацией? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Отправите письмо с рекомендациями, установите фильтр и проведете тренинг
б) Установите фильтр для блокировки подозрительных писем
в) Проведете тренинг по распознаванию фишинговых писем
г) Отправите письмо всем сотрудникам с рекомендациями по проверке писем

Задание №13. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
В вашем распоряжении имеется система обнаружения вторжений (IDS), которая постоянно генерирует предупреждения о подозрительном трафике. Однако ваша команда не уверена, действительно ли эти предупреждения указывают на реальные угрозы. Как вы будете действовать дальше? ***(оцениваемые знания, умения, компетенции: У3, У10, З6, ПК. 2.2, ПК. 2.3, ПК2.6).***
а) Проигнорируете предупреждения, пока не получите подтверждение угрозы
б) Увеличите чувствительность системы, чтобы получать больше предупреждений
в) Проведёте дополнительное расследование каждого предупреждения, чтобы определить, является ли оно истинной угрозой
г) Отключите систему до тех пор, пока не сможете подтвердить угрозу

Задание №14. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие области применения программно-аппаратных комплексов являются

наиболее популярными? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Телекоммуникации

б) Безопасность и видеонаблюдение

в) Медицина и биотехнологии

г) Все вышеперечисленные

Задание №15. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Какие инновации внедряются в современные программно-аппаратные комплексы? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Облачные технологии

б) Виртуализация

в) Автономные системы

г) Все вышеперечисленные

Задание №16. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

. Какие критерии важны при выборе программно-аппаратного комплекса? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***

а) Производительность

б) Совместимость с существующими системами

в) Стоимость владения и обслуживания

Задание №17. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

Ваша компания решила перейти на использование облачной платформы для хранения и обработки данных. Какие меры предосторожности вы предусмотрите? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6).***

а) Шифрование данных при передаче и хранении

б) Регулярные аудиты безопасности

в) Соглашения об уровне обслуживания (SLA) с поставщиком услуг

г) Шифрование данных при передаче и хранении, регулярные аудиты безопасности, соглашения об уровне обслуживания (SLA) с поставщиком услуг

Задание №18. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов

В процессе модернизации комплекса вы решили интегрировать новые устройства IoT (Интернет вещей). Какие меры безопасности вы предусмотрите? ***(оцениваемые знания, умения, компетенции: У5, У4, З1, З2, З3, ПК. 2.2, ПК. 2.4, ПК2.6)***

а) Ограничение доступа к устройствам IoT, шифрование данных, регулярное

обновление прошивки устройств IoT
б) Шифрование данных, передаваемых устройствами IoT
в) Регулярное обновление прошивки устройств IoT
г) Ограничение доступа к устройствам IoT

Задание №19. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие критерии важны при выборе программно-аппаратного комплекса? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
а) Производительность
б) Совместимость с существующими системами
в) Стоимость владения и обслуживания
г) Все вышеперечисленные

Задание №20. Выберите правильные вариант ответов и обведите кружочками буквы правильных ответов
Какие проблемы могут возникать при внедрении программно-аппаратных комплексов? ***(оцениваемые знания, умения, компетенции: У1, У2, У3, У8, У4,У9, У10, З1, З2, З5, ПК. 2.2, ПК. 2.4, ПК2.1).***
а) Несовместимость с существующей инфраструктурой
б) Недостаточная квалификация персонала
в) Высокие затраты на внедрение и поддержку
г) Все вышеперечисленные

Ключи ответов

Номер задания	Правильный ответ	
	1 вариант	2 вариант
1	г	г
2	г	б
3	а,б,в	г
4	а,б,в	б
5	г	г
6	б	г
7	г	г
8	г	а,б,в
9	б	а,б,в
10	г	г
11	г	г
12	г	а
13	в	в
14	г	г
15	а,б,в	г
16	г	а,б,в

17	г	г
18	г	а
19	а,б,в	г
20	а,б,в	г

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-10 баллов	2 (неудовлетворительно)	0-50%	низкий
11-13 баллов	3 (удовлетворительно)	51-65%	базовый
14-17 баллов	4 (хорошо)	66-85%	повышенный
18-20 баллов	5 (отлично)	86-100%	высокий

2.2. Практикоориентированные задания.

Задание № 1.

Текст задания.

Промышленное предприятие (условно ОАО «Маяк») специализируется на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную и складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным и финансовым вопросам.

Инструкция.

1. Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт
- разработанная система видеонаблюдения административной зоны;
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 2.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАДАНИЙ

Задание № 1

Текст задания.

Вы работаете руководителем отдела информационных технологий в крупной международной корпорации. Компания занимается производством высокотехнологичного оборудования и имеет филиалы в нескольких странах. Недавно в вашей организации произошел инцидент, связанный с утечкой конфиденциальной информации, что привело к финансовым потерям и репутационным рискам. В связи с этим руководство поставило перед вами задачу пересмотреть политику информационной безопасности и внедрить соответствующие стандарты для минимизации рисков повторения подобных ситуаций.

Вам необходимо разработать план внедрения стандартов безопасности, который будет соответствовать международным требованиям и учитывать специфику деятельности вашей компании. Рассмотрите следующие аспекты:

1. Выбор стандарта безопасности
2. Процессы и процедуры
3. Ресурсы и обучение:
4. Оценка эффективности
5. Интеграция с существующими системами

Ответьте на вопросы:

Какие инструменты и технологии могут быть использованы для автоматизации процессов соответствия стандартам?

Как будет организована работа с внешними подрядчиками и поставщиками в контексте новых стандартов безопасности?

Какие меры предосторожности необходимо принять для защиты интеллектуальной собственности компании?

Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 2

Текст задания.

Вы руководитель отдела информационных технологий в крупной международной корпорации. Компания занимается производством высокотехнологичного оборудования и имеет филиалы в нескольких странах. Недавно в вашей организации произошел инцидент, связанный с утечкой конфиденциальной информации, что привело к финансовым потерям и репутационным рискам. Руководство поручило вам пересмотреть политику информационной безопасности и внедрить соответствующие стандарты для минимизации рисков повторения подобных ситуаций.

Вам необходимо разработать план внедрения стандартов безопасности, который будет соответствовать международным требованиям и учитывать специфику деятельности вашей компании. Рассмотрите следующие аспекты:

1. Выбор стандарта безопасности:
2. Процессы и процедуры:
3. Ресурсы и обучение:
4. Оценка эффективности:
5. Интеграция с существующими системами:

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.

2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 3

Вы являетесь главным специалистом по информационной безопасности в крупной энергетической компании. Ваша организация эксплуатирует автоматизированную систему управления технологическим процессом (АСУ ТП), которая контролирует работу электростанций и распределительных сетей. Система включает в себя множество компонентов, начиная от датчиков и исполнительных механизмов, заканчивая серверами и рабочими станциями операторов.

Недавно в вашей компании был зафиксирован инцидент, связанный с несанкционированным доступом к одной из подсистем АСУ ТП. Злоумышленник смог изменить настройки некоторых параметров, что могло привести к аварийной ситуации. К счастью, инцидент был вовремя обнаружен, и последствия удалось минимизировать. Однако руководство компании требует принятия срочных мер по повышению уровня защищённости всей системы.

Вам необходимо разработать план мероприятий по защите автоматизированной системы от потенциальных угроз. Учтите следующие аспекты:

1. Анализ уязвимостей
2. Меры по защите от несанкционированного доступа
3. Шифрование и аутентификация
4. Мониторинг и обнаружение аномалий
5. План реагирования на инциденты
6. Обучение персонала.

Ответьте на вопросы:

1. Какие стандарты безопасности применимы к АСУ ТП в энергетике?
2. Какие аппаратные и программные средства можно использовать для защиты системы?
3. Как можно обеспечить бесперебойную работу системы даже в условиях кибератаки?

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт

- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание № 4

Вы работаете экспертом по информационной безопасности в крупной телекоммуникационной компании. В последнее время ваша компания столкнулась с рядом инцидентов, связанных с дестабилизацией работы ключевых объектов защиты. Эти инциденты включают в себя атаки на сетевую инфраструктуру, попытки проникновения в базы данных и нарушение работы серверов. Руководство компании обеспокоено этими событиями и поручило вам разработать план противодействия подобным угрозам.

Разработайте комплексный план по выявлению, оценке и нейтрализации дестабилизирующих воздействий на объекты защиты компании. Ваш план должен включать следующие разделы:

1. Идентификация и классификация угроз:
2. Анализ уязвимостей.
3. Разработка мер защиты.
4. Организация мониторинга и реагирования.
5. Обучение и повышение квалификации персонала.

Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 5

Текс задания. Вы являетесь руководителем службы информационной безопасности в крупной финансовой организации. Ваша организация хранит и обрабатывает большие объемы конфиденциальной информации, включая персональные данные клиентов, финансовые отчеты и коммерческую тайну. Недавнее исследование показало, что существует высокий риск несанкционированного доступа к этой информации из-за недостатков в существующих мерах защиты.

Вам необходимо разработать план мероприятий по улучшению программно-аппаратной защиты информации от несанкционированного доступа. План должен включать:

1. Анализ текущего состояния системы защиты:
2. Определение приоритетов:
3. Разработка комплекса мер:
4. Планирование внедрения:
5. Оценка эффективности:

Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.

2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 6

Текст задания.

Вы являетесь ведущим инженером по информационной безопасности в компании, специализирующейся на разработке и эксплуатации автономных автоматизированных систем (ААС). Эти системы широко используются в промышленности, транспорте и других сферах, где требуется высокая надежность и безопасность. Недавно было обнаружено, что одна из ваших ААС подверглась кибератаке, в результате которой была нарушена нормальная работа системы. Это привело к значительным экономическим потерям и репутационному ущербу для компании.

Вам необходимо разработать комплекс мер по защите автономных автоматизированных систем от кибератак и других видов деструктивного воздействия. Рассмотрите следующие аспекты:

1. Классификация угроз:
2. Анализ уязвимостей:
3. Разработка защитных мер:
4. Мониторинг и реагирование:
5. Обучение и подготовка персонала:

Ответьте на вопросы

1. Какие международные стандарты и рекомендации можно использовать для обеспечения безопасности ААС?
2. Как можно гарантировать безопасность ААС в условиях быстро меняющегося ландшафта угроз?
3. Какие инновационные технологии могут быть применены для повышения уровня защиты ААС?

Инструкция.

Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 7

Текст задания.

Вы являетесь разработчиком программного обеспечения в компании, специализирующейся на создании коммерческих продуктов. Ваша команда работает над проектом, который содержит уникальные алгоритмы и технологии, представляющие высокую ценность для бизнеса. Руководство компании обеспокоено возможностью утечки интеллектуальной собственности и требует принять меры для защиты программного кода от обратного инжиниринга и нелегального копирования.

Вам необходимо разработать стратегию защиты программного продукта от изучения и модификации. Рассмотрите следующие аспекты:

1. Методы защиты:
2. Выбор инструментов:
3. Процесс внедрения:
4. Оценка эффективности:
5. Обратная связь и поддержка:

Ответьте на вопросы

1. Какие юридические меры можно принять для дополнительной защиты интеллектуальной собственности?

2. Как учесть требования законодательства разных стран при распространении продукта?

3. Какие этические аспекты стоит учитывать при выборе методов защиты?

Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 8

Текст задания.

Вы являетесь руководителем отдела информационной безопасности в компании, занимающейся разработкой специализированного программного обеспечения для промышленных предприятий. Ваша продукция включает в себя как программные продукты, так и базу данных с конфиденциальной информацией. В последние месяцы участились случаи несанкционированного копирования и распространения вашего ПО и данных, что наносит значительный финансовый ущерб компании.

Вам необходимо разработать комплекс мер по защите программ и данных от несанкционированного копирования. Рассмотрите следующие аспекты:

4. Классификация угроз:
5. Методы защиты:
6. Выбор инструментов:
7. Процесс внедрения:
8. Оценка эффективности:

Ответьте на вопросы:

1. Какие юридические меры можно принять для дополнительной защиты интеллектуальной собственности?

2. Как учесть требования законодательства разных стран при распространении продукта?

3. Какие этические аспекты стоит учитывать при выборе методов защиты?

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт

- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание № 9

Текст задания.

Вы являетесь руководителем отдела информационной безопасности в компании, занимающейся разработкой специализированного программного обеспечения для промышленных предприятий. Ваша продукция включает в себя как программные продукты, так и базу данных с конфиденциальной информацией. В последние месяцы участились случаи несанкционированного копирования и распространения вашего ПО и данных, что наносит значительный финансовый ущерб компании.

Вам необходимо разработать комплекс мер по защите программ и данных от несанкционированного копирования. Рассмотрите следующие аспекты:

4. Классификация угроз:
5. Методы защиты:
6. Выбор инструментов:
7. Процесс внедрения:
8. Оценка эффективности:

Ответьте на вопросы:

1. Какие юридические меры можно принять для дополнительной защиты интеллектуальной собственности?

2. Как учесть требования законодательства разных стран при распространении продукта?

3. Какие этические аспекты стоит учитывать при выборе методов защиты?

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт

- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание № 10

Текст задания.

Вы являетесь специалистом по информационной безопасности в крупной финансовой организации. Ваша компания активно использует разнообразные аппаратные средства для идентификации и аутентификации пользователей, такие как смарт-карты, токены и биометрические устройства. Однако в последнее время участились случаи мошенничества, когда злоумышленники получают доступ к системам, используя украденные или поддельные аппаратные ключи. Руководство компании поручило вам проанализировать ситуацию и предложить меры по усилению защиты.

Вам необходимо разработать план мероприятий по повышению надежности и безопасности аппаратных средств идентификации и аутентификации пользователей. Рассмотрите следующие аспекты:

4. Классификация угроз:
5. Методы защиты:
6. Выбор инструментов:

7. Процесс внедрения:
8. Оценка эффективности:

Ответьте на вопросы

1. Какие юридические меры можно принять для предотвращения мошенничества с аппаратными средствами?
2. Как можно обеспечить соблюдение сотрудниками политики безопасности?
3. Какие этические аспекты стоит учитывать при выборе методов защиты?

Инструкция.

Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему безопасности по заданию.

Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Критерии оценивания практикоориентированных заданий

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по профессиональному модулю, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» – студент в полном объеме освоил программный материал по профессиональному модулю, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» – студент обнаруживает знание и понимание основных положений программного материала по профессиональному модулю, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по профессиональному модулю, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

4. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия,2019 – 352 с.

2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А., М.: ИЦ Академия, 2019 – 272 с.

Дополнительные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013 – 172 с.

4. Организационно-правовое обеспечение Информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие -Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.

9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

16. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

21. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

22. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

24. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

25. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

26. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

27. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

28. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

29. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

30. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

31. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

32. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

34. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

35. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

36. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

37. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

38. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

39. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

40. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

41. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

42. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

43. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

45. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

46. Номенклатура показателей качества. Ростехрегулирование, 2005.

47. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

48. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

49. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

50. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

51. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

53. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

54. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

55. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

56. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.

57. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

58. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

59. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с.

4. Интерфейсы периферийных устройств – https://intuit.ru/studies/courses/92/92/lecture/28396

5. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2

6. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146

7. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074

8. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240

9. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158

10. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157

Цифровая образовательная среда СПО PROFобразование:

- Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование,

Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87882 (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:
IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/