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

Комплект контрольно-оценочных средств

по

МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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:
Дешина И.А., 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 **МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**, 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) предназначены для контроля и оценки образовательных достижений обучающихся по МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

КОС включают типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, и (или) практического опыта, характеризующих этапы формирования компетенций в процессе освоения образовательной программы для проведения текущего контроля успеваемости обучающихся и организации промежуточной аттестации в форме **экзамена**.

КОС разработан на основании рабочей программы **МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**.

1.2 Планируемые результаты освоения междисциплинарного курса:

В результате освоения междисциплинарного курса обучающийся должен **уметь**:

У1 - осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 - организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 - осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 - производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 - настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 - обеспечивать работоспособность, обнаруживать и устранять неисправности

В результате освоения междисциплинарного курса обучающийся должен **знать**:

З1 - состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 - принципы разработки алгоритмов программ, основных приемов программирования;

З3 - модели баз данных;

З4 - принципы построения, физические основы работы периферийных устройств

З5 - теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 - порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 - принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

В результате освоения междисциплинарного курса обучающийся должен **иметь практический опыт:**

ПО1 - установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

ПО2 - администрирование автоматизированных систем в защищенном исполнении

ПО3 - эксплуатация компонентов систем защиты информации автоматизированных систем

ПО4 - диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

Профессиональные и общие компетенции, которые формируются при изучении междисциплинарного курса:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных

общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Планируемые личностные результаты освоения рабочей программы междисциплинарного курса:

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

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 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

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

ЛР 8. Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.

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.

ЛР 12. Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.

1.3 Контроль и оценка результатов освоения междисциплинарного курса

Таблица 1

Код и наименование профессиональных и общих компетенций, формируемые в рамках междисциплинарного курса	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями	тестирование, экспертное наблюдение выполнения практических работ, экзамен

требованиями эксплуатационной документации.	эксплуатационной документации	
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экспертное наблюдение выполнения практических работ, экзамен
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения практических работ, экзамен
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экспертное наблюдение выполнения практических работ, экзамен

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения междисциплинарного курса для проведения текущего контроля успеваемости обучающихся

2.1. Тестовые задания

Раздел 1. Разработка защищенных автоматизированных (информационных) систем.

Задание № 1. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК 1.1, ПК 1.2)*

Что является основной целью защиты информационных систем?

1. Увеличение скорости обработки данных.
2. Обеспечение конфиденциальности, целостности и доступности информации.
3. Снижение стоимости оборудования.
4. Упрощение интерфейса пользователя.
5. Увеличение объема хранимых данных.

Задание № 2. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК 1.1, ПК 1.2)*

Как называется комплекс средств, различных устройств и мебели, предназначенных для решения различных информационных задач?

1. Специальное рабочее место
2. Рабочее место пользователя
3. Автоматизированное место пользователя
4. Автоматизированное рабочее место
5. Программно-аппаратный комплекс

Задание № 3. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК 1.1, ПК 1.2)*

К какому виду обеспечения относятся модели оптимизации:

1. Техническое
2. Программное
3. Построения моделей
4. Математическое
5. Организационное

Задание № 4. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 31, 32, У1, ПК 1.1, ПК 1.2)*

На какой стадии жизненного цикла определяется архитектура системы:

1. анализ и формирование требований
2. проектирование,
3. разработка
4. тестирование
5. внедрение

Задание № 5. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 31, 32, У1, ПК 1.1, ПК 1.2)*

При какой модели жизненного цикла на выходе получается много самостоятельно работающих программ?

1. спиральная модель
2. каскадная модель
3. инкрементная модель
4. мультипрограммная модель
5. последовательная модель

Задание № 6. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 33, 34, У3, ПК 1.2, ПК 1.3)*

Какой метод управления доступом подразумевает использование списка, содержащего набор субъектов и ассоциированных с ними типов доступа?

1. дискреционный метод
2. идентификационный метод
3. ролевой метод
4. мандатный метод
5. классификационный метод

Задание № 7. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 33, 34, У3, ПК 1.2, ПК 1.3)*

Какая виртуализация использует программную имитацию ресурсов физического сервера?

1. программная виртуализация
2. аппаратная виртуализация
3. виртуализация рабочих столов
4. виртуализация контейнеров
5. виртуализация физических ресурсов

Задание № 8. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, ПК 1.2, ПК 1.3)*

Определение пространства, в котором исключено неконтролируемое пребывание работников является частью:

1. защиты от внешних воздействий
2. контроля и управления физическим доступом
3. организации контролируемой зоны
4. защиты программно-аппаратных средств
5. исключения несанкционированного просмотра

Задание № 9. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З5, У4, ПК 1.2, ПК 1.3)*

К какой группе методов относится создание замкнутого пространства:

1. организационные методы
2. аппаратно-программные методы
3. методы контроля доступа
4. методы идентификации пользователей
5. протоколирование

Задание № 10. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, ПК 1.2, ПК 1.3)*

Какой уровень защищенности персональной информации требует создания специального подразделения, ответственного за безопасность персональных данных:

1. 1 уровень
2. 2 уровень
3. 3 уровень
4. 4 уровень
5. 5 уровень

Задание № 11. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, З7, ПК 1.2, ПК 1.3)*

Что такое система обнаружения вторжений (IDS)?

1) Система, которая блокирует все входящие подключения к сети.
2) Система, которая отслеживает сетевой трафик и выявляет подозрительную активность.

3) Система, которая автоматически удаляет вредоносные файлы с компьютера.
4) Система, которая шифрует данные для защиты от утечек.
5) Система, которая создает резервные копии данных.

Задание № 12. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, З7, ПК 1.2, ПК 1.3)*
Какой тип анализа использует IDS для обнаружения атак на основе известных шаблонов?

1) Анализ аномалий.
2) Поведенческий анализ.
3) Сигнатурный анализ.
4) Статистический анализ.
5) Эвристический анализ.

Задание № 13. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, З7, ПК 1.2, ПК 1.3)*
Какая из перечисленных характеристик относится к системе предотвращения вторжений (IPS), но не к системе обнаружения вторжений (IDS)?

1) Возможность отслеживать сетевой трафик.
2) Способность блокировать подозрительные действия в реальном времени.
3) Возможность создавать отчеты о подозрительной активности.
4) Способность анализировать журналы событий.
5) Возможность шифровать данные.

Задание № 14. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З5, У3, З6, ПК 1.2, ПК 1.3)*
Что такое "уровень защищенности персональных данных" в ИСПДн?

1) Количество пользователей, имеющих доступ к системе.
2) Скорость обработки данных в системе.
3) Количество резервных копий данных.
4) Степень защищенности данных от несанкционированного доступа, определяемая на основе классификации.
5) Уровень квалификации сотрудников, работающих с системой.

Задание № 15. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З5, У3, З6, ПК 1.2, ПК 1.3)*

Какая из перечисленных характеристик является обязательной для ИСПДн?

1) Наличие журнала учета действий с персональными данными.
2) Возможность интеграции с социальными сетями.
3) Поддержка мобильных устройств.
4) Использование искусственного интеллекта.
5) Наличие облачного хранилища.

Задание № 16. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК 1.1, ПК 1.2)*

Сопоставьте понятия из левого столбца с их определениями из правого столбца.

1. Информационная система (ИС)	А. Совокупность мер, направленных на защиту информации от несанкционированного доступа, утечек и повреждений.
2. Угроза информационной безопасности	Б. Программное или аппаратное средство, предназначенное для предотвращения несанкционированного доступа к данным.
3. Защита информации	В. Событие или действие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.
4. Межсетевой экран (Firewall)	Г. Автоматизированная система для сбора, обработки, хранения и передачи информации.
5. Криптография	Д. Наука о методах обеспечения конфиденциальности и аутентичности информации с использованием шифрования.

Запишите ответ:

1	2	3	4	5

Задание № 17. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З1, З2, У1, ПК 1.1, ПК 1.2)*

Сопоставьте компоненты информационной системы с их функциями.

1. Аппаратное обеспечение	А. Обеспечивает взаимодействие пользователя с системой через интерфейсы.
2. Программное обеспечение	Б. Включает серверы, компьютеры, сетевые устройства и другие физические элементы.
3. Данные	В. Защищает информацию от несанкционированного доступа и утечек.

4. Пользователи	Г. Обрабатывает, хранит и управляет данными.
5. Системы защиты информации	Д. Информация, которая хранится и обрабатывается в системе.

Запишите ответ:

1	2	3	4	5

Задание № 18. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.3, ПК 1.4)*

Сопоставьте типы угроз информационной безопасности с их характеристиками.

1. Вредоносное ПО (вирусы)	А. Программы, которые собирают информацию о пользователе без его согласия.
2. Фишинг	Б. Программы, которые повреждают или уничтожают данные.
3. Шпионское ПО	В. Попытка получения конфиденциальной информации через поддельные письма или сайты.
4. DDoS-атака	Г. Попытка получения конфиденциальной информации через поддельные письма или сайты.
5. Социальная инженерия	Д. Манипулирование людьми для получения доступа к информации.

Запишите ответ:

1	2	3	4	5

Задание № 19. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.3, ПК 1.4)*

Сопоставьте методы защиты информации с их описаниями.

1. Шифрование	А. Разделение данных на части и хранение их в разных местах.
2. Резервное копирование	Б. Преобразование данных в нечитаемый формат для защиты от несанкционированного доступа.
3. Аутентификация	В. Создание копий данных для восстановления в случае потери.
4. Разделение данных	Г. Проверка подлинности пользователя или системы.
5. Аудит	Д. Регулярная проверка и анализ событий в системе для выявления нарушений.

Запишите ответ:

1	2	3	4	5

Задание № 20. Прочитайте текст и установите последовательность. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

Расположите следующие этапы в правильной последовательности, чтобы отразить логику защиты информации от угроз.

А) Реагирование на инциденты и восстановление данных.

Б) Мониторинг и анализ событий безопасности.

В) Идентификация угроз и уязвимостей.

Г) Установка и настройка средств защиты (например, антивирусов и брандмауэров).

Д) Регулярное обновление программного обеспечения и систем.

Запишите ответ:

1	2	3	4	5

Ключи ответов

Номер задания	Правильный ответ
1	2
2	4
3	4
4	2
5	3
6	1
7	1
8	3
9	1
10	4
11	2
12	3
13	2
14	4
15	1
16	1-Г, 2-В, 3-А, 4-Б, 5-Д
17	1-Б, 2-Г, 3-Д, 4-А, 5-В
18	1-Б, 2-В, 3-А, 4-Г, 5-Д
19	1-Б, 2-В, 3-Г, 4-А, 5-Д
20	1-В 2-Г 3-Д 4-Б 5-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
0-10 баллов	2 (неудовлетворительно)	0-50%	низкий
11-13 баллов	3 (удовлетворительно)	55-65%	базовый
14-17 баллов	4 (хорошо)	70-85%	повышенный
18-20 баллов	5 (отлично)	90-100%	высокий

Раздел 2. Эксплуатация защищенных автоматизированных систем.

Задание № 1. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Какой метод анализа информационной инфраструктуры позволяет выявить слабые места в системе безопасности?

1) Тестирование производительности системы.
2) Аудит безопасности.
3) Опрос пользователей.
4) Анализ финансовых затрат на систему.
5) Проверка удобства интерфейса.

Задание № 2. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Какая из перечисленных мер является наиболее эффективной для защиты данных в автоматизированной системе?

1) Регулярное обновление программного обеспечения.
2) Увеличение объема оперативной памяти.
3) Установка дополнительных мониторов для сотрудников.
4) Использование сложных паролей и двухфакторной аутентификации.
5) Проведение тренингов по повышению квалификации.

Задание № 3. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)*

Какая из перечисленных задач является основной для системного администратора автоматизированной системы?

1) Разработка нового программного обеспечения.
2) Проведение маркетинговых исследований.
3) Обеспечение стабильной работы системы и ее компонентов.
4) Обучение пользователей работе с офисными программами.
5) Написание технической документации для пользователей.

Задание № 4. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)*

Какое средство защиты информации используется для контроля и фильтрации сетевого трафика?

1) Антивирусное программное обеспечение.
2) Межсетевой экран (брандмауэр).
3) Система резервного копирования.
4) Программа для шифрования данных.
5) Система управления базами данных.

Задание № 5. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Какой метод аудита информационной безопасности подготавливает информационную систему к сертификации?

1) экспертный
2) анализ соответствия стандартам
3) анализ требований ГОСТ
4) активный
5) метод предсертификации

Задание № 6. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

К какой функциональной группе администрирования АС относится регулярное резервное копирования данных?

1) управление конфигурацией;
2) управление производительностью;
3) управление использованием ресурсов;
4) управление обработкой неисправностей;
5) управление безопасностью

Задание № 7. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З5, З6, У5, У6, ПК 1.3, ПК 1.4)*

Какая трудовая функция выполняется инженером по защите информации?

1) Разработка модели угроз безопасности информации
2) Разработка отчетных документов и разделов технических заданий
3) Установка обновлений программного обеспечения АС
4) Разработка модели нарушителя в автоматизированных системах

5) Уничтожение (стирание) информации на машинных носителях

Задание № 8. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 35, 36, У5, У6, ПК 1.3, ПК 1.4)*
К какой группе мер защиты относится исключение несанкционированного доступа к гипервизору?

1) Меры по контролю (анализу) защищенности информации
2) Управление доступом субъектов доступа
3) Идентификация и аутентификация
4) Меры по обнаружению (предотвращению) вторжений
5) Меры по защите среды виртуализации

Задание № 9. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 35, 36, У5, У6, ПК 1.3, ПК 1.4)*
Как называются испытания, при которых проходит проверка работы АИС на действующем оборудовании?

1) действующие испытания
2) опытные испытания
3) опытная эксплуатация
4) основные испытания
5) проверка правильности работы АИС

Задание № 10. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 35, 36, У5, У6, ПК 1.3, ПК 1.4)*
Что такое "разграничение доступа" в контексте информационной безопасности?

1) Ограничение прав доступа пользователей к устройствам и данным в зависимости от их роли и обязанностей.
2) Предоставление всем пользователям одинаковых прав доступа к устройствам.
3) Полное блокирование доступа к устройствам для всех пользователей.
4) Удаление ненужных учетных записей пользователей.
5) Увеличение скорости доступа к устройствам.

Задание № 11. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: 31, 32, У1, У2, ПК 1.1, ПК 1.2)*

В каком разделе технического задания указываются требования к операционным системам?

1) Требования к функциональным характеристикам
2) Требования к надежности
3) Условия эксплуатации
4) Требования к составу и параметрам технических средств
5) Требования к информационной и программной совместимости

Задание № 12. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З4, З5, У4, У5, ПК 1.2, ПК 1.3)*

Что такое "Release Printing" (печать с подтверждением)?

1) Печать документов без предварительного просмотра.
2) Печать документов с автоматическим шифрованием.
3) Печать документов с использованием облачных технологий.
4) Печать документов только после авторизации пользователя на устройстве.
5) Печать документов с высокой скоростью.

Задание № 13. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З4, З5, У4, У5, ПК 1.2, ПК 1.3)*

Какой из перечисленных методов помогает предотвратить несанкционированный доступ к напечатанным документам?

1) Установка принтера в отдельном помещении с ограниченным доступом.
2) Использование принтеров с функцией цветной печати.
3) Регулярное обновление драйверов принтера.
4) Увеличение объема оперативной памяти принтера.
5) Проведение тренингов для пользователей.

Задание № 14. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З4, З6, У4, У7, ПК 1.2, ПК 1.4)*

Что такое "контроль целостности" в контексте информационной безопасности?

1) Обеспечение высокой скорости работы системы.
2) Увеличение объема хранимых данных.
3) Проверка соответствия данных и программного обеспечения установленным стандартам.
4) Регулярное обновление программного обеспечения.
5) Проведение тренингов для пользователей.

Задание № 15. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. *(оцениваемые знания, умения, компетенции: З4, З6, У4, У7, ПК 1.2, ПК 1.4)*

Что такое "замкнутая программная среда"?

1) Среда, в которой все программы работают независимо друг от друга.
2) Среда, в которой доступ к программам и данным строго контролируется и ограничивается.
3) Среда, в которой используются только облачные технологии.
4) Среда, в которой все программы обновляются автоматически.
5) Среда, в которой пользователи имеют неограниченный доступ ко всем ресурсам.

Задание № 16. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

Сопоставьте понятия информационной безопасности с их характеристиками.

1. Аудит безопасности	А. Постоянное наблюдение за сетевым трафиком для выявления подозрительной активности.
2. Мониторинг сетевого трафика	Б. Проверка системы на наличие известных уязвимостей и слабых мест.
3. Анализ журналов событий	В. Исследование записей в журналах для обнаружения аномалий или нарушений.
4. Сканирование уязвимостей	Г. Использование заранее определенных шаблонов для обнаружения известных угроз.
5. Сигнатурный анализ	Д. Комплексная проверка системы на соответствие требованиям безопасности.

Запишите ответ:

1	2	3	4	5

Задание № 17. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З3, З4, У3, У4, ПК 1.3, ПК 1.4)*

Установите соответствие между методом мониторинга/аудита и его описанием.

1. Анализ журналов событий (логов)	А. Проверка соответствия системы требованиям стандартов и нормативных документов.
2. Аномальный (поведенческий) анализ	Б. Сканирование сети и поиск уязвимостей в автоматическом режиме.
3. Анализ соответствия стандартам	В. Анализ записей журналов работы системы для выявления подозрительной активности.
4. Внутренний аудит безопасности	Г. Оценка поведения пользователей и сетевого трафика для выявления аномалий.
5. Сканирование уязвимостей	Д. Комплексная проверка защиты информационной системы внутренними специалистами.

Запишите ответ:

1	2	3	4	5

Задание № 18. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З5, З6, У5, У6, ПК 1.3, ПК 1.4)*

Установите соответствие между технологиями и их задачами.

1. Резервное копирование (Backup)	А. Защита данных при передаче через открытые сети.
2. Шифрование данных	Б. Создание копий данных для восстановления при сбое.
3. Биометрическая аутентификация	В. Идентификация пользователя по уникальным биологическим признакам.
4. Система мониторинга безопасности	Г. Постоянный контроль событий и анализ логов.
5. Логирование	Д. Регистрация действий пользователей и системных процессов.

Запишите ответ:

1	2	3	4	5

Задание № 19. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З5, З6, У6, У7, ПК 1.3, ПК 1.4)*

Сопоставьте типы угроз информационной безопасности с их характеристиками.

1. Антивирусное ПО	А. Проверка и фильтрация данных на сетевом уровне.
2. Система контроля доступа (DLP)	Б. Защита от вредоносного ПО и вирусов.
3. Брандмауэр (Firewall)	В. Обнаружение и предотвращение утечек данных.
4. VPN (Виртуальная частная сеть)	Г. Мониторинг и выявление подозрительной активности.
5. IDS/IPS (Система обнаружения вторжений)	Д. Г. Шифрование интернет-трафика для защиты данных.

Запишите ответ:

1	2	3	4	5

Задание № 20. Прочитайте текст и установите последовательность. Ответ запишите в таблицу. *(оцениваемые знания, умения, компетенции: З5, З6, У5, У6, ПК 1.3, ПК 1.4)*

Расположите следующие этапы в правильной последовательности, чтобы отразить логику защиты информации от несанкционированного доступа.

А) Обновление и улучшение мер защиты на основе анализа инцидентов.

Б) Установка и настройка систем аутентификации и авторизации.

В) Регулярный аудит и мониторинг доступа к информации.

Г) Реализация механизмов шифрования данных.

Д) Идентификация и классификация информационных ресурсов.

Запишите ответ:

1	2	3	4	5

Ключи ответов

Номер задания	Правильный ответ
1	2
2	4
3	3
4	2
5	5
6	4
7	4
8	5
9	3
10	1
11	5
12	4
13	1
14	3
15	2
16	1-Д 2-А 3-В 4-Б 5-Г
17	1-В 2-Г 3-А 4-Д 5-Б
18	1-Б 2-А 3-В 4-Г 5-Д
19	1-Б 2-В 3-А 4-Д 5-Г
20	1-Д 2-Б 3-Г 4-В 5-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**
0-10 баллов	2 (неудовлетворительно)	0-50%	низкий
11-13 баллов	3 (удовлетворительно)	55-65%	базовый
14-17 баллов	4 (хорошо)	70-85%	повышенный
18-20 баллов	5 (отлично)	90-100%	высокий

2.2. Вопросы для устного опроса.

Тема 1.1. Основы информационных систем как объекта защиты.

Вопросы:

1. Что понимается под информационной системой как объектом защиты? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
2. Какие процессы происходят в информационной системе? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
3. Какие предъявляются требования к информационной системе? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Тема 1.2. Жизненный цикл автоматизированных систем

Вопросы:

1. Какие основные стадии включает жизненный цикл автоматизированных систем? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
2. Какую роль играет этап анализа требований в жизненном цикле автоматизированных систем? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
3. Какие методы и подходы используются на этапе проектирования автоматизированных систем? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Тема 1.3. Угрозы безопасности информации в автоматизированных системах

Вопросы:

1. Что понимается под угрозой безопасности информации в автоматизированных системах? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
2. Приведите примеры основных типов угроз (естественные, искусственные, внутренние, внешние). *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*
3. Какие угрозы безопасности информации могут возникать из-за ошибок в проектировании или настройке автоматизированных систем? *(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК 1.1, ПК 1.2)*

Тема 1.4. Основные меры защиты информации в автоматизированных системах

Вопросы:

1. Какие основные принципы защиты информации в автоматизированных системах вы знаете? *(оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)*
2. Объясните, как принципы конфиденциальности, целостности и доступности реализуются на практике. (оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)
3. Какие технические меры защиты информации можно использовать в автоматизированных системах? (оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)

4. Какие организационные меры защиты информации необходимо применять в автоматизированных системах? (оцениваемые знания, умения, компетенции: З2, З3, У2, У3, ПК 1.1, ПК 1.2)

Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении

Вопросы:

1. Какие основные этапы включает процесс эксплуатации автоматизированных систем в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
2. Какие меры безопасности должны быть реализованы при настройке автоматизированной системы в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
3. Какие действия необходимо выполнить при выводе автоматизированной системы из эксплуатации? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

Тема 1.6. Защита информации в распределенных автоматизированных системах

Вопросы:

1. Какие особенности распределенных автоматизированных систем создают дополнительные риски для безопасности информации? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
2. Как организовать управление доступом в распределенных автоматизированных системах? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
3. Как осуществляется мониторинг и предотвращение атак в распределенных автоматизированных системах? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

Тема 1.7. Особенности разработки информационных систем персональных данных

Вопросы:

1. Какие этапы проектирования информационных систем персональных данных требуют особого внимания с точки зрения безопасности? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
2. Какие технические меры защиты персональных данных должны быть реализованы в информационных системах? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*
3. Какие организационные меры необходимо предусмотреть при разработке информационных систем персональных данных? *(оцениваемые знания, умения, компетенции: З2, З3, З4, У3, У4, ПК 1.2, ПК 1.3)*

Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.

Вопросы:

1. Какие основные задачи решаются в процессе эксплуатации автоматизированных систем в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какие меры безопасности должны быть реализованы при повседневной эксплуатации автоматизированных систем в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие особенности необходимо учитывать при обновлении программного обеспечения в автоматизированных системах в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.2. Администрирование автоматизированных систем

Вопросы:

1. Какие основные задачи выполняет администратор автоматизированных систем? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какие инструменты и технологии используются для администрирования автоматизированных систем? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие меры безопасности должен предпринимать администратор для защиты автоматизированных систем от угроз? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении

Вопросы:

1. Какие основные обязанности возлагаются на персонал, эксплуатирующий автоматизированные системы в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какие меры безопасности должен соблюдать персонал при работе с автоматизированными системами в защищенном исполнении? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Как организовать взаимодействие между различными группами персонала (администраторы, операторы, специалисты по безопасности) при эксплуатации защищенных автоматизированных систем? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.4. Защита от несанкционированного доступа к информации

Вопросы:

1. Какие основные методы и технологии используются для защиты от несанкционированного доступа к информации? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

2. Как организовать управление доступом в информационной системе для предотвращения несанкционированного доступа? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие организационные меры необходимо предпринять для защиты от несанкционированного доступа к информации? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.5. СЗИ от НСД

Вопросы:

1. Какие основные функции выполняют средства защиты информации от несанкционированного доступа (СЗИ от НСД)? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какие требования предъявляются к средствам защиты информации от НСД в соответствии с нормативными документами? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие особенности необходимо учитывать при внедрении и эксплуатации СЗИ от НСД в информационных системах? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях

Вопросы:

1. Какие основные средства защиты информации применяются в компьютерных сетях? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какие меры необходимо предпринять для защиты данных при передаче по компьютерным сетям? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие действия необходимо выполнить при обнаружении сетевой атаки или утечки данных? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Тема 2.7. Документация на защищаемую автоматизированную систему

Вопросы:

1. Какие виды документации должны быть разработаны для защищаемой автоматизированной системы? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
2. Какую роль играет техническое задание (ТЗ) при разработке защищаемой автоматизированной системы? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*
3. Какие разделы должны быть включены в политику информационной безопасности защищаемой автоматизированной системы? *(оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК 1.3, ПК 1.4)*

Критерии оценивания ответов на вопросы

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, 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 междисциплинарному курсу, 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 междисциплинарному курсу, 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 междисциплинарному курсу, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

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

Для проведения промежуточной аттестации в форме экзамена используются настоящие контрольно-оценочные средства для оформления экзаменационных билетов Количество экзаменационных билетов должно превышать количество студентов на 3.

ПРИМЕР ОФОРМЛЕНИЯ БИЛЕТА

Министерство образования Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Алексеевский колледж»

МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

семестр 7 курс 4

группа 841

Билет № **1**

1. Понятие автоматизированной (информационной) системы. Отличительные черты АИС. Примеры областей применения АИС.
2. Практическое задание …

Преподаватель: _____ И.А. Дешина
(подпись)

3.1. Перечень вопросов.

1. Понятие автоматизированной (информационной) системы. Отличительные черты АИС. Примеры областей применения АИС. (оцениваемые знания, умения, компетенции: З1, З3, У1, У3, ПК 1.1, ПК 1.2)

2. Процессы в АИС. Требования к АИС: гибкость, надежность, эффективность, безопасность. (оцениваемые знания, умения, компетенции: З1, З3, У1, У3, ПК 1.1, ПК 1.2)

3. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС. (оцениваемые знания, умения, компетенции: З2, З3,, У4, У5, ПК 1.2, ПК 1.3)

4. Модели жизненного цикла АИС. (оцениваемые знания, умения, компетенции: З2, З3,, У4, У5, ПК 1.2, ПК 1.3)

5. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. (оцениваемые знания, умения, компетенции: З1, З2, З3, У2, У4, ПК 1.1, ПК 1.2)

6. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. (оцениваемые знания, умения, компетенции: З1, З2, З3, У2, У4, ПК 1.1, ПК 1.2)

7. Потенциальные угрозы безопасности в автоматизированных системах. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, ПК 1.1, ПК 1.2)

8. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, ПК 1.1, ПК 1.2)

9. Методы оценки опасности угроз. Банк данных угроз безопасности информации. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, ПК 1.1, ПК 1.2)

10. Понятие уязвимости угрозы. Классификация уязвимостей. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, ПК 1.1, ПК 1.2)

11. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах. (оцениваемые знания, умения, компетенции: З4, З5, З6, У5, У6, ПК 1.2, ПК 1.3)

12. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.

(оцениваемые знания, умения, компетенции: З4, З5, З6, У5, У6, ПК 1.2, ПК 1.3)

13. Идентификация и аутентификация субъектов доступа и объектов доступа. (оцениваемые знания, умения, компетенции: З2, З3, З7, У3, У4, ПК 1.1, ПК 1.2)

14. Управление доступом субъектов доступа к объектам доступа. (оцениваемые знания, умения, компетенции: З2, З3, З7, У3, У4, ПК 1.1, ПК 1.2)

15. Обнаружение (предотвращение) вторжений. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, У3, ПК 1.2, ПК 1.3)

16. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения. (оцениваемые знания, умения, компетенции: З1, З2, З3, У1, У2, У3, ПК 1.3, ПК 1.4)

17. Защита технических средств. (оцениваемые знания, умения, компетенции: З4, З5, З6, З7, У4, У5, У6, ПК 1.3, ПК 1.4)

18. Защита информационной системы, ее средств, систем связи и передачи данных. (оцениваемые знания, умения, компетенции: З4, З5, З6, З7, У4, У5, У6, ПК 1.3, ПК 1.4)

19. Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. (оцениваемые знания, умения, компетенции: З6, У3, У5, ПК. 1.1, ПК.1.4)

20. Требования по защите персональных данных, в соответствии с уровнем защищенности. (оцениваемые знания, умения, компетенции: З6, У3, У5, ПК. 1.1, ПК.1.4)

21. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. (оцениваемые знания, умения, компетенции: З1, З3, У1, У5, ПК. 1.2)

22. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. (оцениваемые знания, умения, компетенции: З1, З5, З6, З7, У3, У5, У6, ПК 1.2, ПК 1.3)

23.23. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. (оцениваемые знания, умения, компетенции: З3, З7, У2, У4, ПК. 1.1, ПК.1.4)

24. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. (оцениваемые знания, умения, компетенции: З4, З5, З6, З7, У3, У5, У6, ПК 1.3, ПК 1.4)

25. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. (оцениваемые знания, умения, компетенции: З7, У5, У6, ПК 1.3, ПК 1.4)

26. Классификация автоматизированных систем. Требования по защите информации от НСД для АС. (оцениваемые знания, умения, компетенции: З3, З7, У2, У4, ПК. 1.1, ПК.1.4)

27. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях. (оцениваемые знания, умения, компетенции: З4, З7, У2, У3, ПК. 1.1, ПК.1.4)

28. Основные эксплуатационные документы защищенных автоматизированных систем. (оцениваемые знания, умения, компетенции: З3, З7, У2, У4, ПК. 1.1, ПК.1.4)

3.2. Перечень практических заданий.

1. Проведите сравнение традиционных и автоматизированных

информационных технологий. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

2. Приведите классификацию информационных систем. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

3. Охарактеризуйте виды угроз информационной безопасности. Приведите примеры. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

4. Охарактеризуйте виды угроз по характеру происхождения угроз информационной безопасности. Приведите примеры умышленных и естественных факторов. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

5. Проведите анализ защищенности объекта защиты информации по следующим направлениям: виды возможных угроз, характер происхождения угроз, источники появления угроз.(оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

6. Разработайте памятку по безопасной работе с автоматизированной системой. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

7. Разработайте политику информационной безопасности для автоматизированной системы. (оцениваемые знания, умения, компетенции: З1, З2, У1, У2, ПК. 1.1, ПК.1.2)

8. Произведите настройку аудита локальной системы на ПК. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

9. Настройте политику паролей в Windows/Linux, обеспечивающую безопасность учётных записей. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

10. Произведите ограничение доступ пользователей к критически важным файлам и папкам. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

11. Проведите аудит учетных записей пользователей на наличие избыточных прав. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

12. Настройте сбор логов событий Windows/Linux с сохранением их на удалённый сервер. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

13. Проанализируйте журналы событий Windows/Linux на предмет подозрительной активности. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

14. Проверьте систему Windows/Linux на попытки несанкционированного входа. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

15. Настройте права доступа к общим ресурсам для пользователей и групп. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

16. Проведите аудит политик групповой безопасности и их соответствие требованиям защиты. (оцениваемые знания, умения, компетенции: З2, З3, У3, У4, ПК. 1.2, ПК.1.3)

17. Настройте брандмауэр (iptables, Windows Firewall) для блокировки нежелательного трафика. (оцениваемые знания, умения, компетенции: З4, З5, З6, У4, У5, ПК. 1.3, ПК.1.4)

18. Проведите анализ системы на наличие открытых портов и ненужных сервисов. (оцениваемые знания, умения, компетенции: З4, З5, З6, У4, У5, ПК. 1.3, ПК.1.4)

19. Настройте автоматическое обновление системы и программного обеспечения. (оцениваемые знания, умения, компетенции: З4, З5, З6, У4, У5, ПК. 1.3, ПК.1.4)

20. Обновите все программные компоненты системы до последних версий, чтобы устранить известные уязвимости. (оцениваемые знания, умения, компетенции: З4, З5, З6, У4, У5, ПК. 1.3, ПК.1.4)

21. Настройте антивирусное ПО и проведите сканирование системы. (оцениваемые знания, умения, компетенции: З4, З5, З6, У4, У5, ПК. 1.3, ПК.1.4)

22. Изолируйте потенциально опасное ПО в виртуальной среде (песочнице). (оцениваемые знания, умения, компетенции: З4, З5,зЗ6, У4, У5, ПК. 1.3, ПК.1.4)

23. Проведите анализ установленных программ и удалите ненужные или подозрительные. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

24. Настройте систему резервного копирования системных файлов. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

25. Настройте систему резервного копирования базы данных. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

26. Настройте автоматический бэкап критически важных данных с хранением в защищённом хранилище. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

27. Настройте политику удаления данных, чтобы автоматически удалять устаревшие данные через определенный период. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

28. Создайте план действий при потере данных и протестируйте восстановление после сбоя. (оцениваемые знания, умения, компетенции: З5, З6, З7, У5, У6, ПК. 1.3, ПК.1.4)

Критерии оценивания

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, 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 междисциплинарному курсу, 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 междисциплинарному курсу, 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 междисциплинарному курсу, 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. Эксплуатация автоматизированных (информационных) систем защищённом исполнении (1-е изд.) учебное пособие/Кравченко В.Б. М.: ИЦ Академия, 2018-304 с

Дополнительные источники:

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии - М.: Издательский центр «Академия», 2014.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации - М.: Издательский центр «Академия», 2016.

3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.

4. Мельников Д. Информационная безопасность открытых систем.- М.:Форум, 2013.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание - Питер, 2015.

6. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы - М.: Издательский центр «Академия», 2013.

7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. -М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. - Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. - Саратов : Профобразование, 2019. - 136 с. - ISBN 978-5-4488-0355-0. - Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. URL: https://profspo.ru/books/86210 (дата обращения: 07.09.2020). - Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - https: // www.iprbookshop.ru/102192.html

Веб-система для организации дистанционного обучения и управления им:

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