Учреждение профессионального образования
«Колледж Казанского инновационного университета»
Альметьевский филиал

УТВЕРЖДЕНА
в составе Основной
образовательной программы –
программы подготовки специалистов среднего звена
протокол № 6 от «28» августа 2024 г.

Фонд оценочных средств

ОП.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

программы подготовки специалистов среднего звена
по специальности
09.02.07 Информационные системы и программирование
(на базе основного общего образования)
Срок получения СПО по ППССЗ – 3 г.10 мес.

Форма обучения – очная

Присваиваемая квалификация
Программист

Альметьевск 2024

Фонд оценочных средств по дисциплине ОП.14 Информационная безопасность программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование разработан на основе рабочей программы дисциплины

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Фонд оценочных средств (ФОС) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу дисциплины ОП.14 Информационная безопасность.

ФОС включает оценочные материалы для проведения текущего и итогового контроля.

ФОС разработан на основании:

– ООП программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование;

– рабочей программы учебной дисциплины ОП.14 Информационная безопасность.

2. ПОКАЗАТЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ФОРМЫ И МЕТОДЫ КОНТРОЛЯ И ОЦЕНКИ

Изучение дисциплины «Информационная безопасность» обеспечивает формирование у выпускников по специальности 09.02.07 Информационные системы и программирование следующих общих компетенций (ОК) и профессиональных компетенций(ПК). В результате освоения учебной дисциплины у обучающегося должны быть сформированы следующие компетенции:

Код ПК, ОК	**Умения**	**Знания**	**Практический опыт**
1	*2*	*3*	*4*
ОК1	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составить план действия; определить необходимые ресурсы;	- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и	

Код ПК, ОК	Умения	Знания	Практический опыт
1	*2*	*3*	*4*
	- владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).	смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.	
ОК2	- определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.	- номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации.	
ОК5	- грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе.	- особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.	
ПК4.4	- использовать методы защиты программного обеспечения компьютерных систем; - анализировать риски и характеристики качества программного обеспечения; - выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.	- основные средства и методы защиты компьютерных систем программными и аппаратными средствами.	- обеспечивать защиту программного обеспечения компьютерных систем программными средствами

3. ОЦЕНОЧНЫЕ СРЕДСТВА (ФОРМЫ) ТЕКУЩЕГО КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Содержание учебного материала	Элементы результата обучения			
	ОК1	ОК2	ОК5	ПК4.4
Тема 1. Введение в информационную безопасность		УО Д Т ПЗ		
Тема 2. Угрозы информационной безопасности	УО Д ПЗ	УО Д ПЗ	УО Д ПЗ	
Тема 3. Система управления информационной безопасностью предприятия	УО Д ПЗ	УО Д ПЗ	УО Д ПЗ	УО Д ПЗ
Тема 4. Нормативно-правовые основы информационной безопасности в РФ		УО Д ПЗ	УО Д ПЗ	УО Д ПЗ
Тема 5. Стандарты в области информационной безопасности		УО Д ПЗ	УО Д ПЗ	
Тема 6. Криптографическая защита информации		УО Д ПЗ	УО Д ПЗ	УО Д ПЗ
Тема 7. Антивирусная безопасность информации		УО Д ПЗ	УО Д ПЗ	УО Д ПЗ
Тема 8. Сетевая безопасность информации		УО Д ПЗ	УО Д ПЗ	УО Д ПЗ
Тема 9. Основные программно-технические меры защиты информации		УО Д ПЗ	УО Д ПЗ	УО Д ПЗ

УО – устный опрос
ПЗ – практическое занятие
Д – доклад
Т – тест

4. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

4.1. Текущий контроль

4.1.1. Задания для практических работ по темам

Тема 1. Введение в информационную безопасность

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Перечень вопросов:

1. Информационная безопасность общества
2. Концепция информационной безопасности
3. Защищаемая информация и информационные ресурсы
4. Понятие информационной безопасности
5. Составляющие информационной безопасности

ЗАДАНИЕ 1. Устный опрос

Цель: Выявления уровня знаний в ходе изучения одной из темы/раздела, их систематизация и степень сформированности понимания.

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

ЗАДАНИЕ 2. Подготовка доклада

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Выступление с докладом является дополнительным видом работ для формирования повышенного уровня освоения компетенции и предполагает самостоятельный подбор студентом темы для доклада по согласованию с преподавателем, либо выбор из предложенных тем.

Регламент выступления – 5-7 минут.

Цель выступления с докладом: Раскрыть сущность и особенности изучаемого теоретического вопроса, либо темы.

Задание: Тема может быть выбрана студентов как самостоятельно, так и по рекомендации преподавателя. Как правило, самостоятельная работа над темой дает хорошие результаты по закреплению изученного материала, и более глубокому изучению проблемы.

Тематика докладов

1. Концепция информационной безопасности.
2. Проблема информационной безопасности общества.
3. Информационная безопасность и уровни ее обеспечения.

Критерии оценки

Оценка «**отлично**» – Выполнены все требования к написанию и защите доклада. Обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, даны правильные ответы на дополнительные вопросы.

Оценка «**хорошо**» – Выполнены основные требования к написанию доклада и к его защите, но при этом допущены недочеты, в частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объем, на дополнительные вопросы при защите даны неполные ответы.

Оценка «**удовлетворительно**» – Имеются существенные отступления от требований к написанию доклада, в частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

ЗАДАНИЕ 3. Тестовые задания

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Тест – Совокупность стандартизированных заданий, результат выполнения которых позволяет измерить знания и умения испытуемого.

Цель тестового задания – Контроль знаний освоения дисциплины, получить ответ от испытуемого, на основе которого сделать вывод о его знаниях,

представлениях из определенной области содержания дисциплины.

Задание: Перечень вопросов**,** соответствующих содержанию дисциплины. Обучающемуся предлагается ответить на вопросы закрытой формы тестов, включающей в себя от 2 до 7 вариантов ответа, из которых один или несколько являются верными.

Инструкция: Выберите один или несколько правильных ответа из предложенных.

Критерии оценки – соответствие ответов обучающихся ключу теста:

Оценка «**отлично**» – если обучающийся правильно выполнил на 25 тестовых заданий в отведенное время.

Оценка «**хорошо»** – если обучающийся правильно выполнил от 19 до 24 тестовых заданий в отведенное время.

Оценка **«удовлетворительно»** – если обучающийся правильно выполнил от 14 до 18 тестовых заданий в отведенное время.

Оценка «**неудовлетворительно**» – ставится в случае выполнения менее 14 тестовых заданий.

Вопросы тестирования

1. **Утечка информации – это** (выберите один из трех вариантов ответа):

а) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;

б) ознакомление постороннего лица с содержанием секретной информации;

в) потеря, хищение, разрушение или неполучение переданных данных.

2. **Под изоляцией и разделением** (требование к обеспечению информационной безопасности) понимают – (выберите один из двух вариантов ответа):

а) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов);

б) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп.

3. **К аспектам информационной безопасности относятся –** (выберите несколько из пяти вариантов ответа):

а) дискретность;

б) целостность;

в) конфиденциальность;

г) актуальность;

д) доступность.

4. **Линейное шифрование –** (выберите один из трех вариантов ответа):

а) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу;

б) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому;

в) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами.

5. **Угроза – это** (выберите один из двух вариантов ответа):

а) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов;

б) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов.

6. **Под информационной безопасностью понимают –** (выберите один из трех вариантов ответа):

а) защиту от несанкционированного доступа;

б) защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера;

в) защиту информации от компьютерных вирусов.

7. **Что такое криптография?** (выберите один из трех вариантов ответа):

а) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом;

б) область доступной информации;

в) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом.

8. **Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется** (выберите один из четырех вариантов ответа):

а) кодируемой;

б) шифруемой;

в) недостоверной;

г) защищаемой.

9. **Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие – это** (выберите один из четырех вариантов ответа):

а) текст;

б) данные;

в) информация;

г) пароль.

10. **Организационные угрозы подразделяются** на – (выберите несколько из четырех вариантов ответа):

а) угрозы воздействия на персонал;

б) физические угрозы;

в) действия персонала;
г) несанкционированный доступ.

11. **Виды технической разведки (по месту размещения аппаратуры) –** (выберите несколько из семи вариантов ответа):
а) космическая;
б) оптическая;
в) наземная;
г) фотографическая;
д) морская;
е) воздушная;
ж) магнитометрическая.

12. **Основные группы технических средств ведения разведки** (выберите несколько из пяти вариантов ответа):
а) радиомикрофоны;
б) фотоаппараты;
в) электронные «уши»;
г) дистанционное прослушивание разговоров;
д) системы определения местоположения контролируемого объекта.

13. **Разновидности угроз безопасности –** (выберите несколько из шести вариантов ответа):
а) техническая разведка;
б) программные;
в) программно-математические;
г) организационные;
д) технические;
е) физические.

14. **Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется** (выберите один из четырех вариантов ответа):
а) угрозой;
б) опасностью;
в) намерением;
г) предостережением.

15. **Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?** (выберите один из четырех вариантов ответа):
а) операционной системы, системного программного обеспечения;
б) операционной системы, системного программного обеспечения и системы управления базами данных;
в) операционной системы, системы управления базами данных;
г) системного программного обеспечения и системы управления базами данных.

16. **Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов**

угроз безопасности объектам защиты называется (выберите один из четырех вариантов ответа):

а) системой угроз;

б) системой защиты;

в) системой безопасности;

г) системой уничтожения.

17. **К видам защиты информации относятся** (выберите несколько из четырех вариантов ответа):

а) правовые;

б) морально-этические;

в) юридические;

г) административно-организационные.

18. **К методам защиты от несанкционированного доступа относятся** (выберите несколько из пяти вариантов ответа):

а) разделение доступа;

б) разграничение доступа;

в) увеличение доступа;

г) ограничение доступа;

д) аутентификация и идентификация.

19. **Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется** (выберите один из четырех вариантов ответа):

а) политикой информации;

б) защитой информации;

в) политикой безопасности;

г) организацией безопасности.

20. **Выделите группы, на которые делятся средства защиты информации** (выберите один из трех вариантов ответа):

а) физические, аппаратные, программные, криптографические, комбинированные;

б) химические, аппаратные, программные, криптографические, комбинированные;

в) физические, аппаратные, программные, этнографические, комбинированные;

21. **Какие законы существуют в России в области компьютерного права?** (выберите несколько из шести вариантов ответа):

а) о государственной тайне;

б) об авторском праве и смежных правах;

в) о гражданском долге;

г) о правовой охране программ для ЭВМ и БД;

д) о правовой ответственности;

е) об информации, информационных технологиях и о защите информации.

22. **В чем заключается основная причина потерь информации, связанной с персональным компьютером?** (выберите один из трех вариантов ответа):

а) с глобальным хищением информации;

б) с появлением интернета;

в) с недостаточной образованностью в области безопасности.

23. **Что такое несанкционированный доступ?** (выберите один из пяти вариантов ответа):

а) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

б) создание резервных копий в организации;

в) правила и положения, выработанные в организации для обхода парольной защиты;

г) вход в систему без согласования с руководителем организации;

д) удаление не нужной информации.

24. **Что такое аутентификация?** (выберите один из пяти вариантов ответа):

а) проверка количества переданной и принятой информации;

б) нахождение файлов, которые изменены в информационной системе не санкционированно;

в) проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа);

г) определение файлов, из которых удалена служебная информация;

д) определение файлов, из которых удалена служебная информация.

25. **Кодирование информации –** (выберите один из двух вариантов ответа):

а) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.;

б) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом.

Ключ к тестовым заданиям

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

Тема 2. Угрозы информационной безопасности

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Перечень вопросов:

1. Угрозы безопасности информации
2. Классификация угроз безопасности информации
3. Виды потенциальных угроз безопасности информации
4. Факторы информационной безопасности

ЗАДАНИЕ 1. Устный опрос

Цель: Выявления уровня знаний в ходе изучения одной из темы/раздела, их систематизация и степень сформированности понимания.

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

ЗАДАНИЕ 2. Подготовка доклада

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Выступление с докладом является дополнительным видом работ для формирования повышенного уровня освоения компетенции и предполагает самостоятельный подбор студентом темы для доклада по согласованию с преподавателем, либо выбор из предложенных тем.

Регламент выступления – 5-7 минут.

Цель выступления с докладом: Раскрыть сущность и особенности изучаемого теоретического вопроса, либо темы.

Задание: Тема может быть выбрана студентов как самостоятельно, так и по рекомендации преподавателя. Как правило, самостоятельная работа над темой дает хорошие результаты по закреплению изученного материала, и более глубокому изучению проблемы.

Тематика докладов

1. Классификация угроз безопасности информации.
2. Антропогенные источники угроз безопасности информации.
3. Техногенные источники угроз безопасности информации.
4. Стихийные источники угроз безопасности информации.

Критерии оценки

Оценка «**отлично**» – Выполнены все требования к написанию и защите доклада. Обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, даны правильные ответы на дополнительные вопросы.

Оценка «**хорошо**» – Выполнены основные требования к написанию доклада и к его защите, но при этом допущены недочеты, в частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объем, на дополнительные вопросы при защите даны неполные ответы.

Оценка «**удовлетворительно**» – Имеются существенные отступления от требований к написанию доклада, в частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Тема 3. Система управления информационной безопасностью предприятия

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Перечень вопросов:

1. Определение управления информационной безопасностью.
2. Концептуальная модель информационной безопасности.
3. Организация системы обеспечения информационной безопасности.
4. Функциональная структура управления информационной безопасностью.

ЗАДАНИЕ 1. Устный опрос

Цель: Выявления уровня знаний в ходе изучения одной из темы/раздела, их систематизация и степень сформированности понимания.

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

ЗАДАНИЕ 2. Подготовка доклада

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Выступление с докладом является дополнительным видом работ для формирования повышенного уровня освоения компетенции и предполагает самостоятельный подбор студентом темы для доклада по согласованию с преподавателем, либо выбор из предложенных тем.

Регламент выступления – 5-7 минут.

Цель выступления с докладом: Раскрыть сущность и особенности изучаемого теоретического вопроса, либо темы.

Задание: Тема может быть выбрана студентов как самостоятельно, так и по рекомендации преподавателя. Как правило, самостоятельная работа над темой дает хорошие результаты по закреплению изученного материала, и более глубокому изучению проблемы.

Тематика докладов

1. Документальное обеспечение системы управления информационной безопасностью предприятия.
2. Жизненный цикл документального обеспечения системы управления информационной безопасностью предприятия.
3. Поддержка системы управления информационной безопасностью со стороны руководства предприятия.
4. Мониторинг системы управления информационной безопасностью.

Критерии оценки

Оценка «**отлично**» – Выполнены все требования к написанию и защите доклада. Обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, даны правильные ответы на дополнительные вопросы.

Оценка «**хорошо**» – Выполнены основные требования к написанию доклада и к его защите, но при этом допущены недочеты, в частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объем, на дополнительные вопросы при защите даны неполные ответы.

Оценка «**удовлетворительно**» – Имеются существенные отступления от требований к написанию доклада, в частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Тема 4. Нормативно-правовые основы информационной безопасности в Российской Федерации.

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4.

Перечень вопросов:

1. Нормативно-правовые основы информационной безопасности.
2. Основные положения законодательных актов РФ в области информационной безопасности и защиты информации
3. Ответственность за нарушения в сфере информационной безопасности.

ЗАДАНИЕ 1. Устный опрос

Цель: Выявления уровня знаний в ходе изучения одной из темы/раздела, их систематизация и степень сформированности понимания.

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

ЗАДАНИЕ 2. Подготовка доклада

Проверяемые результаты обучения: ОК01, ОК02, ПК4.4

Выступление с докладом является дополнительным видом работ для формирования повышенного уровня освоения компетенции и предполагает самостоятельный подбор студентом темы для доклада по согласованию с преподавателем, либо выбор из предложенных тем.

Регламент выступления – 5-7 минут.

Цель выступления с докладом: Раскрыть сущность и особенности изучаемого теоретического вопроса, либо темы.

Задание: Тема может быть выбрана студентов как самостоятельно, так и по рекомендации преподавателя. Как правило, самостоятельная работа над темой дает хорошие результаты по закреплению изученного материала, и более глубокому изучению проблемы.

Тематика докладов

1. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».
2. Основные положения Федерального закона «О персональных данных».

Критерии оценки

Оценка «**отлично**» – Выполнены все требования к написанию и защите доклада. Обозначена проблема и обоснована ее актуальность, сделан краткий

анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, даны правильные ответы на дополнительные вопросы.

Оценка «**хорошо**» – Выполнены основные требования к написанию доклада и к его защите, но при этом допущены недочеты, в частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объем, на дополнительные вопросы при защите даны неполные ответы.

Оценка «**удовлетворительно**» – Имеются существенные отступления от требований к написанию доклада, в частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Тема 5. Стандарты в области информационной безопасности.

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Перечень вопросов:

1. Содержание основных стандартов по информационной безопасности.
2. Базовые сервисы безопасности в вычислительных сетях.
3. Наиболее эффективные механизмы безопасности.
4. Задачи администрирования средств безопасности.
5. Содержание основных стандартов оценки защищенности автоматизированных систем.

ЗАДАНИЕ 1. Устный опрос

Цель: Выявления уровня знаний в ходе изучения одной из темы/раздела, их систематизация и степень сформированности понимания.

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

ЗАДАНИЕ 2. Подготовка доклада

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Выступление с докладом является дополнительным видом работ для формирования повышенного уровня освоения компетенции и предполагает самостоятельный подбор студентом темы для доклада по согласованию с преподавателем, либо выбор из предложенных тем.

Регламент выступления – 5-7 минут.

Цель выступления с докладом: Раскрыть сущность и особенности изучаемого теоретического вопроса, либо темы.

Задание: Тема может быть выбрана студентов как самостоятельно, так и по рекомендации преподавателя. Как правило, самостоятельная работа над темой дает хорошие результаты по закреплению изученного материала, и более глубокому изучению проблемы.

Тематика докладов

1. Основное содержание оценочного стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
2. Основные стандарты распределенных систем.

Критерии оценки

Оценка «**отлично**» – Выполнены все требования к написанию и защите доклада. Обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, даны правильные ответы на дополнительные вопросы.

Оценка «**хорошо**» – Выполнены основные требования к написанию доклада и к его защите, но при этом допущены недочеты, в частности, имеются неточности в изложении материала, отсутствует логическая

последовательность в суждениях, не выдержан объем, на дополнительные вопросы при защите даны неполные ответы.

Оценка «**удовлетворительно**» – Имеются существенные отступления от требований к написанию доклада, в частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Тема 6. Криптографическая защита информации

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Перечень вопросов:

1. Основные криптографические примитивы
2. Элементарное шифрование
3. Симметричная криптография
4. Асимметричная криптография
5. Электронная подпись и криптографическая хеш-функция
6. Инфраструктура открытых ключей

Критерии оценивания:

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

Тема 7. Антивирусная безопасность информации

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Перечень вопросов:

1. Вредоносное программное обеспечение.
2. Классификация вредоносного программного обеспечения.
3. Классы антивирусных программ.
4. Методы антивирусной защиты информации
5. Классы антивирусных средств защиты информации

6. Функциональные модули антивирусных программ.

7. Управление антивирусной защиты информации.

Критерии оценивания:

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

Тема 8. Сетевая безопасность информации

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Перечень вопросов:

1. Понятие сетевой безопасности

2. Базовая эталонная модель взаимосвязи открытых систем

3. Стек протоколов TCP/IP

4. Средства обеспечения сетевой безопасности

Критерии оценивания:

Оценка «**отлично**» обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» обучающийся не смог ответить на вопрос.

Тема 9. Основные программно-технические меры защиты информации

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Перечень вопросов:

1. Идентификация и аутентификация
2. Управление доступом
3. Протоколирование и аудит
4. Шифрование
5. Контроль целостности
6. Цифровые сертификаты

Критерии оценивания:

Оценка «**отлично**» – обучающийся правильно ответил на вопрос.

Оценка «**хорошо**» – обучающийся при ответе допустил небольшие ошибки.

Оценка «**удовлетворительно**» – ответ обучающегося был с ошибками.

Оценка «**неудовлетворительно**» – обучающийся не смог ответить на вопрос.

3.4. Практические задания

Тема 1. Введение в информационную безопасность

Практическая занятие. Методы поиска и сбора информации.

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Цель практического занятия: Приобретение навыков поиска информации, используя поисковые системы.

Задачи:

1. Поисковые системы. Методика поиска.
2. Рассылки, тематические форумы.
3. Возможности использования иноязычных ресурсов.

Оценка «**отлично**» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути практического занятия.

Оценка «**хорошо»** – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка **«удовлетворительно»** – Задание практического занятия выполнено только частично. Нет понимания сути выполненной работы. Имеются грубые ошибки в выполнении заданий работы.

Тема 2. Угрозы информационной безопасности

Практическое занятие. Анализ рисков информационной безопасности

Проверяемые результаты обучения: ОК01, ОК02, ОК05

Цель практического занятия: Ознакомиться с алгоритмами оценки риска информационной безопасности

Задание:

1. Загрузите ГОСТ Р ИСО/МЭК 13 335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий»

2. Ознакомьтесь с **Приложениями C, D и E** ГОСТ Р ИСО/МЭК 13 335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий».

3. Выберите три различных информационных актива организации (см. вариант).

4. Из **Приложения D** ГОСТ Р ИСО/МЭК 13 335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий» подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением C** ГОСТ Р ИСО/МЭК 13 335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий» напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТ Р ИСО/МЭК 13 335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий» произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Варианты работ

Номер варианта	**Организация**	**Метод оценки риска (см. Приложение Е ГОСТ)**
1	*2*	*3*
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТ)
1	*2*	*3*
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Тема 3. Система управления информационной безопасностью предприятия

Практическое занятие. «Применение программно-аппаратных средств защиты информации»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Приобретение практических навыков по установке и применению СЗИ НСД «Secret Net Studio»

Задание:

1. Установка на виртуальный стенд операционной системы семейства MS Windows

2. Установка на виртуальный стенд операционной системы семейства MS Windows СЗИ НСД «Secret Net Studio» в автономном режиме

3. Настройка механизмов защиты СЗИ НСД «Secret Net Studio» для работы компьютера в автономном режиме

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

Тема 4. Нормативно-правовые основы информационной безопасности в Российской Федерации

Практическое занятие. «Применение средств защиты информации для обеспечения безопасности информации от внутренних угроз утечки информации»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Приобретение практических навыков по установке и применению программного комплекса «Falcongaze SecureTower» для обеспечения безопасности информации от внутренних угроз утечки информации.

Задание:

1. Изучить теоретические вопросы по установке, настройке и работе с программным комплексом Falcongaze SecureTower.

2. Подготовить к работе виртуальный стенд и выполнить практическую работу в соответствии с методическими указаниями к данной практической работе.

3. Получить практические навыки по установке, настройке и работе с программным комплексом Falcongaze SecureTower.

4. Описать принцип работы программного комплекса Falcongaze SecureTower при проведении практической работы на виртуальном стенде.

4. Оформить отчет по выполненной практической работе.

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

Тема 5. Стандарты в области информационной безопасности

Практическое занятие. «Разработка политики информационной безопасности предприятия»

Проверяемые результаты обучения: ОК02, ОК05

Цель практического занятия: Знакомство с основными принципами разработки политики информационной безопасности предприятия, с учетом особенностей его информационной инфраструктуры.

Цель работы: Знакомство с основными принципами разработки политики информационной безопасности предприятия, с учетом особенностей его информационной инфраструктуры.

Задание:

Используя предложенные образцы, разработать политику информационной безопасности предприятия (см. вариант), содержащую следующие основные пункты (приведен примерный план, в который, в случае, необходимости могут быть внесены изменения):

1. Общие положения

1.1. Назначение Политики информационной безопасности предприятия.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности

2.2. Определение вероятного нарушителя

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей

2.4. Основные виды угроз информационной безопасности предприятия

– Классификации угроз

– Основные непреднамеренные искусственные угрозы

– Основные преднамеренные искусственные угрозы

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности предприятия

3.1. Принципы, условия и требования к предприятию и к функционированию системы информационной безопасности

3.2. Основные направления политики предприятия в сфере информационной безопасности

3.3. Планирование мероприятий по обеспечению информационной безопасности предприятия

3.4. Критерии и показатели информационной безопасности предприятия.

4. Мероприятия по реализации мер информационной безопасности предприятия

4.1. Организационное обеспечение информационной безопасности.

– Задачи организационного обеспечения информационной безопасности.

– Подразделения, занятые в обеспечении информационной безопасности.

– Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности предприятия.

– Общие положения.

– Защита информационных ресурсов от несанкционированного доступа.

– Средства комплексной защиты от потенциальных угроз.

– Обеспечение качества в системе безопасности.

– Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности предприятия.

– Правовое обеспечение юридических отношений с работниками предприятия.

– Правовое обеспечение юридических отношений с партнерами Предприятия.

– Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности предприятия

5. Программа создания системы информационной безопасности предприятия

Номер варианта	**Организация**	**Метод оценки риска (см. Приложение Е ГОСТ)**
1	*2*	*3*
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4
9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1

Номер варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТ)
1	*2*	*3*
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

Тема 6. Криптографическая защита информации

Практическое занятие. «Разворачивание центра сертификации на базе Microsoft Certification Authority»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Приобретение навыков работы по развертыванию на предприятии удостоверяющего центра Microsoft Certification Authority

Задание:

1. Подготовка контроллера домена для центра сертификации Microsoft
2. Подготовка веб-сервера для центра сертификации Microsoft
3. Установка корневого центра сертификации Microsoft
4. Установка издающего центра сертификации Microsoft

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

Тема 7. Антивирусная безопасность информации

Практическое занятие: «Установка и развертывание сетевой версии антивирусного продукта Kaspersky Security Center в ЛВС на базе доменов (с использованием средств виртуализации MS Hyper-V)»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Получить практические навыки по установке и развертыванию сетевой версии антивирусного программного продукта Kaspersky Security Center.

Задание:

1. Изучить теоретические вопросы по установке и развертыванию сетевой версии антивирусного программного продукта Kaspersky Security Center.

2. Получить практические навыки по установке и развертыванию сетевой версии антивирусного программного продукта Kaspersky Security Center.

3. Описать принцип организации виртуальной среды при проведении практического занятия на виртуальных стендах.

4. Оформить отчет по выполненному практическому занятию.

5. Письменно ответить на контрольные вопросы к практическому занятию.

Критерии оценки

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

Тема 8. Сетевая безопасность информации

Практическое занятие: «Установка и развертывание ЛВС на базе доменов (с использованием средств виртуализации MS Hyper-V)»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Получить практические навыки по установке и развертыванию локальных вычислительных сетей (с использованием средств виртуализации MS Hyper-V).

Задание:

1. Изучить теоретические вопросы:

– по использованию средств виртуализации при построении ЛВС с применением гипервизора MS Hyper-V;

– по установке, развертыванию и администрированию серверной операционной системы MS Windows Server Data Center 2012 R2 с использованием средств виртуализации MS Hyper-V.

2. Получить практические навыки по установке и развертыванию серверной операционной системы MS Windows Server Data Center 2012 R2 с использованием средств виртуализации MS Hyper-V.

3. Описать принцип организации виртуальной среды при проведении практической работы на виртуальных стендах.

4. Оформить отчет по выполненной практическому заданию.

Критерии оценки

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

Тема 9. Основные программно-технические меры защиты информации

Практическое занятие. «Установка и настройка службы каталогов Microsoft Active Directory»

Проверяемые результаты обучения: ОК01, ОК02, ОК05, ПК4.4

Цель практического занятия: Приобретение практических навыков по установке и настройке службы каталогов Microsoft Active Directory.

Задание:

1. Изучить теоретические вопросы по установке и настройке службы каталогов Microsoft Active Directory.

2. Получить практические навыки по установке и настройке службы каталогов Microsoft Active Directory.

3. Оформить отчет по выполненному практическому занятию.

4. Письменно ответить на контрольные вопросы к практическому занятию.

Критерии оценки

Оценка «отлично» – Задание практического занятия выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненной работы.

Оценка «хорошо» – Задание практического занятия выполнено полностью и правильно, продемонстрировано понимание сути выполненной работы. При выполнении работы могут присутствовать негрубые ошибки.

Оценка «удовлетворительно» – Задание практического занятия выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «неудовлетворительно» – Задание практического занятия не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.

4.2. Промежуточная аттестация

Вопросы к экзамену

1. Концепция информационной безопасности. Составляющие информационной безопасности.
2. Защищаемая информация и информационные ресурсы. Понятие информационной безопасности.
3. Угрозы безопасности информации. Классификация угроз безопасности информации.
4. Виды потенциальных угроз безопасности информации. Факторы информационной безопасности.
5. Определение управления информационной безопасностью. Концептуальная модель информационной безопасности.
6. Организация системы обеспечения информационной безопасности. Функциональная структура управления информационной безопасностью.
7. Правовой статус, структура и основные направления деятельности Совета Безопасности Российской Федерации, основополагающие документы, регламентирующие деятельность Совета Безопасности Российской Федерации в сфере национальной безопасности Российской Федерации официального сайта Совета Безопасности Российской Федерации.
8. Правовая основа, основные угрозы государственной и общественной безопасности Российской Федерации, основные термины и определения, используемые в «Стратегии национальной безопасности Российской Федерации».
9. Правовая основа, основные направления обеспечения информационной безопасности в Российской Федерации, основные термины и определения, используемые в «Доктрина информационной безопасности Российской Федерации».
10. Правовая основа, основные направления развития российских информационных и коммуникационных технологий в Российской

Федерации, основные термины и определения, используемые в «Стратегия развития информационного общества в Российской Федерации».

11. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».
12. Основные положения Федерального закона «О персональных данных».
13. Основное содержание оценочного стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
14. Основные стандарты распределенных систем.
15. Основные криптографические примитивы. Элементарное шифрование.
16. Симметричная криптография.
17. Асимметричная криптография.
18. Электронная подпись и криптографическая хеш-функция.
19 Инфраструктура открытых ключей.
20. Вредоносное программное обеспечение.
21. Классификация вредоносного программного обеспечения.
22. Классы антивирусных программ.
23. Методы антивирусной защиты информации
24. Классы антивирусных средств защиты информации
25. Понятие сетевой безопасности. Базовая эталонная модель взаимосвязи открытых систем.
26. Стек протоколов TCP/IP.
27. Средства обеспечения сетевой безопасности.
28. Идентификация и аутентификация.
29. Управление доступом.
30. Протоколирование и аудит.
31. Шифрование.
32. Контроль целостности.
33. Цифровые сертификаты.

Экзаменационные задания

1. Развернуть на виртуальном стенде контроллер домена на базе серверной операционной системы MS Windows Server Data Center R2
2. Установить и идентифицировать на виртуальном стенде в домене серверной операционной системы MS Windows Server Data Center R2 рабочие станции
3. Развернуть Kaspersky Security Center на виртуальном стенде в домене серверной операционной системы MS Windows Server Data Center R2
4. Установить на виртуальном стенде антивирусные агенты и клиенты Kaspersky Security Center рабочих станций в домене серверной операционной системы MS Windows Server Data Center R2
5. На виртуальном стенде развернуть систему защиты информации от несанкционированного доступа «Secret Net Studio» в автономном режиме

5. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРУ ОЦЕНИВАНИЯ

5.1. Критерии оценивания на экзамене

Оценка «**отлично**» – Задание выполнено полностью и правильно, продемонстрировано глубокое понимание сути выполненного задания. Обучающийся освоил способности эксплуатировать и сопровождать информационные системы и сервисы, а также осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем.

Оценка «**хорошо**» – Задание выполнено полностью и правильно, продемонстрировано понимание сути выполненного задания. При выполнении задания могут присутствовать негрубые ошибки. Обучающийся освоил способности эксплуатировать и сопровождать информационные системы и сервисы, а также осуществлять инсталляцию и настройку параметров программного обеспечения информационных систем.

Оценка «**удовлетворительно**» – Задание выполнено не полностью, но продемонстрировано понимание сути выполненного задания. Обучающийся не в полной мере освоил способности эксплуатировать и сопровождать информационные системы и сервисы.

Оценка «**неудовлетворительно**» – Задание не выполнено, либо выполнено только частично. Нет понимания сути выполненного задания. Имеются грубые ошибки в выполнении задания.