Государственное бюджетное профессиональное образовательное учреждение
«Нижегородский промышленно-технологический техникум»

КОМПЛЕКТ КОНТРОЛЬНО ОЦЕНОЧНЫХ СРЕДСТВ

Профессионального модуля

ПМ03 Применение программно-аппаратных и технических средств защиты информации

специальность
10.02.01 «Организация и технология защиты информации»

Нижний Новгород
2020 г.

Контрольно-оценочные средства профессионального модуля ПМ03 Применение программно-аппаратных и технических средств защиты информации разработаны на основе ФГОС СПО по специальности: 10.02.01 Организация и технология защиты информации и рабочей программы профессионального модуля ПМ03 Применение программно-аппаратных и технических средств защиты информации.

Организация-разработчик:
ГБПОУ «Нижегородский промышленно-технологический техникум»

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
3. ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ
4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

1. ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности по ПМ03 Применение программно-аппаратных и технических средств защиты информации составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ОПОП в целом.

Формой аттестации по профессиональному модулю является экзамен по профессиональному модулю.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

участия в эксплуатации систем и средств защиты информации защищаемых объектов; применения технических средств защиты информации;

выявления возможных угроз информационной безопасности объектов защиты;

уметь:

работать с техническими средствами защиты информации;

работать с защищенными автоматизированными системами; передавать информацию по защищенным каналам связи; фиксировать отказы в работе средств вычислительной техники;

знать:

виды, источники и носители защищаемой информации;

источники опасных сигналов; структуру, классификацию и основные характеристики технических каналов утечки информации;

классификацию технических разведок и методы противодействия им;

методы и средства технической защиты информации;

методы скрытия информации; программно-аппаратные средства защиты информации;

структуру подсистемы безопасности операционных систем и выполняемые ею функции;

средства защиты в вычислительных сетях; средства обеспечения защиты информации в системах управления базами данных; критерии защищенности компьютерных систем;

методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

Профессиональные и общие компетенции

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Результаты (освоенные профессио-нальные компетенции)	**Показатели оценки результата**	***Формы и методы кон-троля и оценки***
ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.	работа с техническими средствами защиты информации; работать с защищенными автоматизированными системами; передавать информацию по защищенным каналам связи;	*Оценка качества выполнения заданий учебной практики* *Отчеты по учебной практике* *Дифференцированный зачет по практике* *экзамен по профессиональному модулю*
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	участие в эксплуатации систем и средств защиты информации защищаемых объектов; применения технических средств защиты информации;	
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	фиксирование отказов в работе средств вычислительной техники;	
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	выявление возможных угроз информационной безопасности объектов защиты;	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	***Формы и методы контроля и оценки***
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.	Проявление интереса при выполнении заданий	*Интерпретация результатов посещения практических занятий и наблюдений за обучающимся*

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Самостоятельность при выполнении заданий на ПК	*Интерпретация результатов наблюдений за обучающимся*
ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	Самостоятельность в принятии решении при выполнении учебных задач	*Интерпретация результатов наблюдений за обучающимися в ходе заданий практики, бесед по результатам выполнения отдельных заданий*
ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	Осуществление	*Оценка использование учебных пособий, Справки и иных источников информации при возникновении затруднений*
ОК 6. Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями.	самостоятельного поиска информации при решении учебных задач	
ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	Использование программ MS Word, Excel, PowePoint, графических редакторов и т.д.	*Оформление портфолио по результатам освоения программы модуля*
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Владение нормами делового общения и речевого этикета в общении с обучающимися, преподавателями, руководством	*Интерпретация результатов наблюдений за обучающимися в ходе выполнения заданий практик*

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.	Проявление ответственности за результат выполнения задания	*Интерпретация результатов проведенной студентом самооценки по результатам практики (на основании портфолио, беседы)*
ОК 10. Применять математический аппарат для решения профессиональных задач.	Определение перспективных задач профессионального развития	*Интерпретация результатов презентации портфолио по результатам освоения программы модуля*
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.	*Оперативность в овладении новыми программны-ми средствами*	*Интерпретация результатов наблюдений за обучающимися в ходе выполнениязаданий практик*
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	*Определение пер-спективных задач профессионального развития*	*Интерпретация результатов наблюдений за обучающимися в ходе выполнения заданий практик*

2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Элемент модуля	Формы промежуточной аттестации	Форма предоставления отчетности
МДК 03.01 Технические методы и средства, технологии защиты информации	Дифференцированный зачет	аттестационная ведомость
МДК 03.02 Программно-аппаратные средства защиты информации	Дифференцированный зачет	аттестационная ведомость
ПМ03 Применение программно-аппаратных и технических средств защиты информации	Экзамен по модулю	аттестационная ведомость

3. ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Текущий контроль

МДК 03.01 Технические методы и средства, технологии защиты информации

№	Вопрос	Уровень освоения	Осваиваемые профессиональные компетенции
1	**1. Физические средства защиты информации. Выберите один из 4 вариантов ответа:** 1) средства, которые реализуются в виде автономных устройств и систем 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу 3) это программы, предназначенные для выполнения функций, связанных с защитой информации 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
2	**2. Технические средства защиты информации. Выберите один из 4 вариантов ответа:** 1) средства, которые реализуются в виде автономных устройств и систем 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу 3) это устройства, предназначенные для выполнения функций, связанных с защитой информации аппаратными средствами 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

3	**3. Утечка информации. Выберите один из 3 вариантов ответа:** 1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу 2) ознакомление постороннего лица с содержанием секретной информации 3) потеря, хищение, разрушение или неполучение переданных данных	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
4	**4. Под изоляцией и разделением (требование к обеспечению ИБ) понимают. Выберите один из 2 вариантов ответа:** 1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов) 2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
5	**5. Виды технической разведки (по месту размещения аппаратуры). выберите несколько из 7 вариантов ответа:** 1) космическая 2) оптическая 3) наземная 4) фотографическая 5) морская 6) воздушная 7) магнитометрическая	**2**	**ПК 3.3. ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

6	**6. Основные группы технических средств ведения разведки. Выберите несколько из 5 вариантов ответа:** 1) радиомикрофоны 2) фотоаппараты 3) электронные "уши" 4) дистанционное прослушивание разговоров 5) системы определения местоположения контролируемого объекта	**2**	**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
7	**7. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется** 1) угрозой; 2) опасностью; 3) намерением; 4) предостережением.	**1**	**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
8	**8. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?** Запишите ответ: _____	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности. ПК 3.3. ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
9	**9. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?** 1) операционной системы, сетевого программного обеспечения 2) операционной системы, сетевого программного обеспечения и системы управления базами данных; 3) операционной системы, системы управления базами данных; 4) сетевого программного обеспечения и системы управления	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности. ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

	базами данных.		**ПК 3.3. Фиксировать отказы в работе средств защиты.**
10	**10. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется** 1) системой угроз; 2) системой защиты; 3) системой безопасности; 4) системой уничтожения.	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
11	**11. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?** Запишите ответ: _____	**3**	**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
12	**12. Выделите группы, на которые делятся средства защиты информации:** 1) физические, аппаратные, программные, криптографические, комбинированные; 2) химические, аппаратные, программные, криптографические, комбинированные; 3) физические, аппаратные, программные, этнографические, комбинированные;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

13	**13.** Надежным средством отвода наведенных сигналов на землю служит Запишите ответ: _____	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.3. Фиксировать отказы в работе средств защиты.**
14	**14. Установите соответствие** **Укажите соответствие для всех 2 вариантов ответа:** 1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи 2) наука скрывающая содержимое секретного сообщения a. стеганография b. криптография	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
15	**15. Контроль доступа к информации обеспечивается последовательным использованием таких методов защиты информации как…** Продолжите _____	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
16	**16. Укажите соответствие для всех 4 вариантов ответа:** 1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет	**2**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

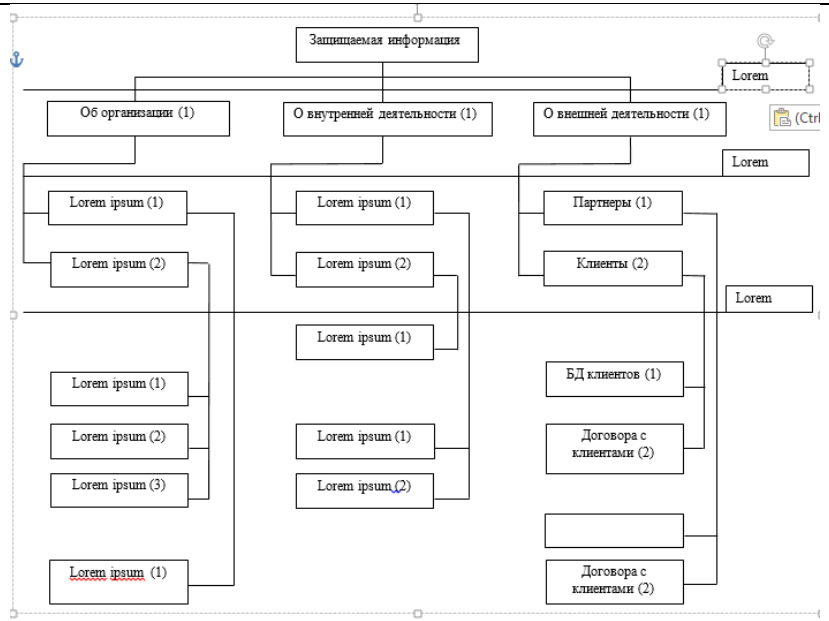
	электромагнитных полей побочного характера и наводок 2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов 3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей 4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии a. защита информации от утечки по акустическому каналу b. Защита информации от утечки по визуально-оптическому каналу c. Защита информации от утечки по электромагнитным каналам d. Защита информации от утечки по материально-вещественному каналу		**ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
17	**17. Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:** 1) собственник информации 2) владелец информации 3) пользователь	**1**	**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

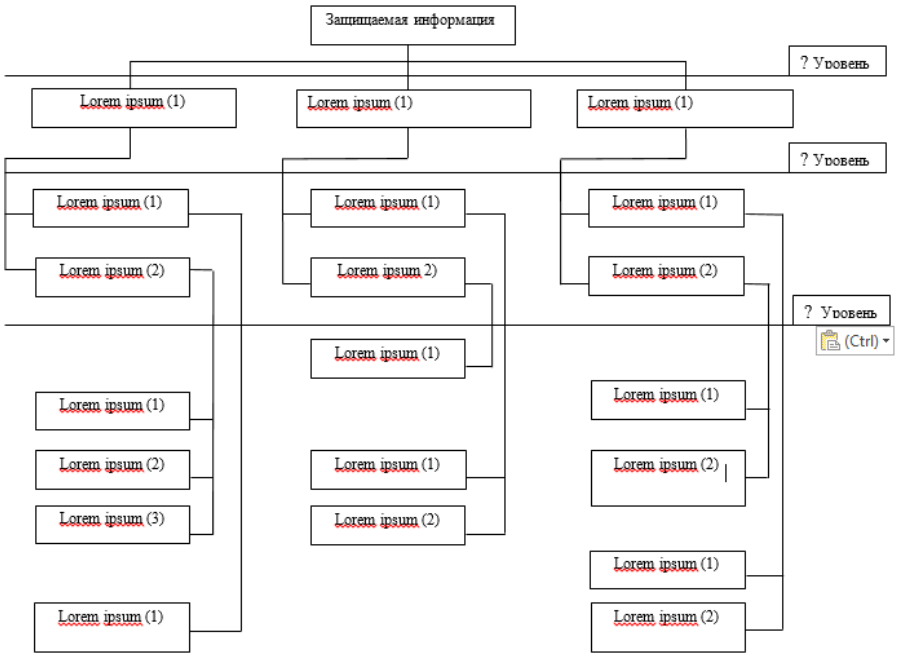
18	**18. Форма допуска, требуемая для работы со сведениями особой важности, является:** 1) первой формой допуска 2) второй формой допуска 3) третьей формой допуска	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
19	**19. Форма допуска, требуемая для работы с совершенно секретными сведениями, является:** 1) первой формой допуска 2) второй формой допуска 3) третьей формой допуска	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
20	**20. Форма допуска, требуемая для работы с секретными сведениями, является:** 1) первой формой допуска 2) второй формой допуска 3) третьей формой допуска	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
21	**21. В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:** 1) каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей 2) каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания 3) каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
22	**22. Противоправные процессы утечки, утраты,**	**1**	

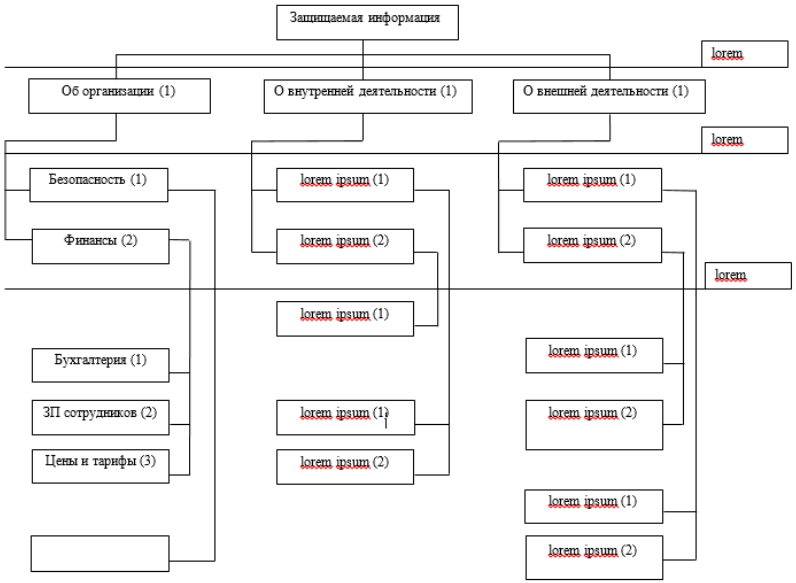
	распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом: 1) незаконного оборота информации 2) взлома информации 3) несанкционированного использования информации		**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
23	**23. Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:** 1) дезинформация 2) легендирование 3) шпионаж	**1**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
24	**24. Какое направление защиты в основном применяется для охраны материальных ценностей?** 1) инженерно-техническая 2) организационно-техническая 3) организационно-распорядительная 4) нормативно-правовая 5) экономическая	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
25	**25. Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?** 1) оптический канал 2) радиоэлектронный канал 3) акустический канал 4) материально-вещественный канал	**1**	**ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

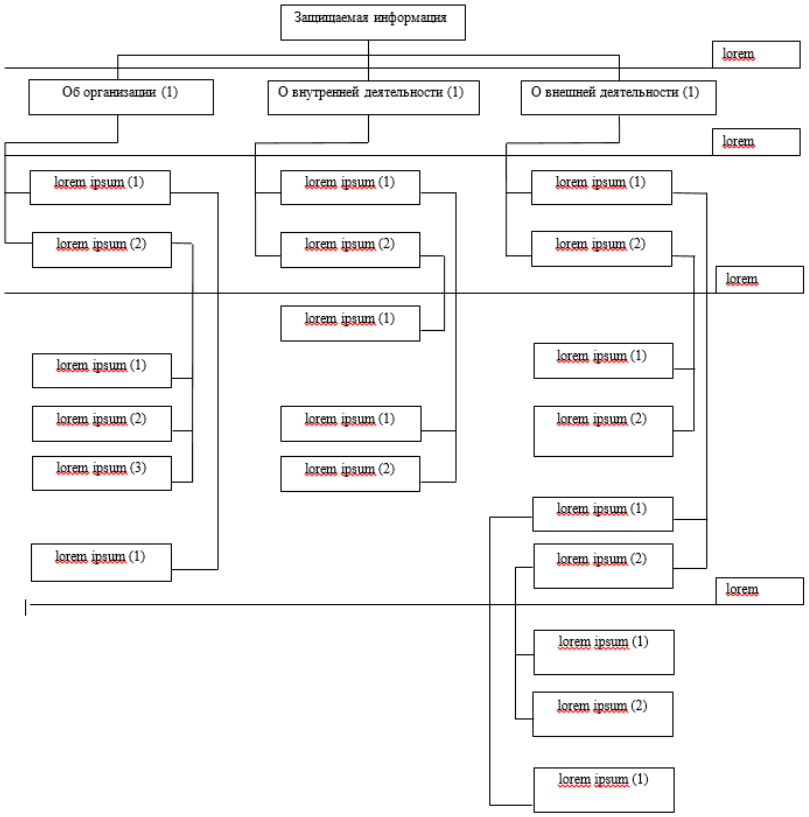
26	**26. Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?** 1) оптический канал 2) радиоэлектронный канал 3) акустический канал 4) материально-вещественный канал	**1**	**ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
27	**27. Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие окружающем пространстве электромагнитную энергию является примером утечки информации:** 1) оптический канал 2) радиоэлектронный канал 3) акустический канал 4) материально-вещественный канал	**1**	**ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
28	**28. Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах** 1) визуально-оптический канал 2) электромагнитный канал 3) виброакустический канал 4) материально-вещественный канал	**1**	**ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
29	**29. Примером какого канала утечки информации служит звук голоса человека?**	**1**	**ПК 3.3. Фиксировать отказы в работе средств защиты.**

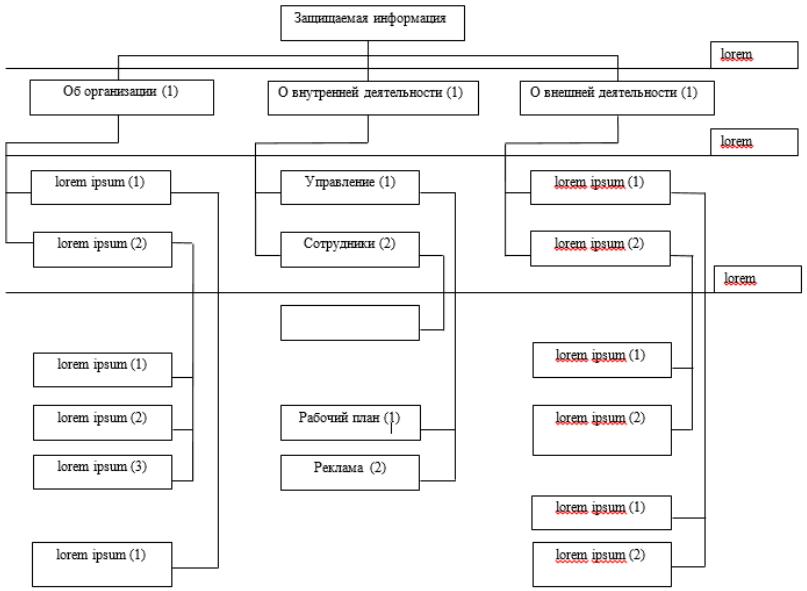
	1) оптический канал 2) радиоэлектронный канал 3) акустический канал 4) материально-вещественный канал		**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
30	**30. По какому признаку делят на классы средства технической разведки (СТР)?** 1) по дальности канала 2) по форме передачи информации 3) по мощности 4) по степени финансирования	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
31	**31. Изучите представленную граф-структуру системы безопасности предприятия.**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

	 **Напишите недостающий элемент защиты информации в правом столбце: _____**		
32	**32. Изучите представленную граф-структуру системы безопасности предприятия.**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

	 **Выпишите цифрами через запятую сверху вниз номера уровней безопасности которые должны быть на схеме**		
33	**33. Изучите представленную граф-структуру системы безопасности предприятия.**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности. ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

	 **Напишите недостающий элемент защиты информации в левом столбце: _____**		**ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
34	**34. Изучите представленную граф-структуру системы безопасности предприятия.**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

	 **Напишите цифрой сколько уровней безопасности представлено на схеме _____**		
35	**35. Изучите представленную граф-структуру системы безопасности предприятия.**	**3**	

	 **Напишите недостающий элемент защиты информации в среднем столбце: _____**		
36	**36. Изучите представленную граф-структуру и часть таблицы данных системы безопасности предприятия.**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

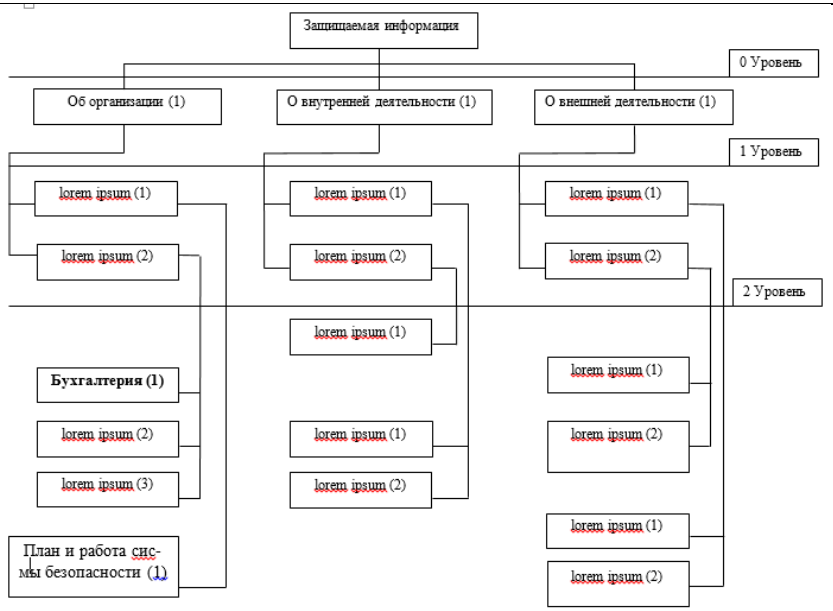


Таблица № 1

Данные о защищаемой информации

№ Эл. инф.	Элементы информации	Гриф КИ	Цена инф, руб.	Носитель информации	Местоположение источника информации
0111	План и работа сис-мы безопасности	КТ	25000	Отчеты, договоры со службой безопасности	Служба безопасности
	бухгалтерия	КТ	5000	HDD ПК, договоры, отчёты	Бухгалтерия/ серверная

Напишите цифрой какой номер элементу информации будет присвоен Бухгалтерии _____

Критерии оценивания:

Тестовое задание рассчитано на 45 мин.

Оценка	**Критерий**
«5»	80 – 100 % от общего числа баллов
«4»	70 - 75 %
«3»	50 - 65 %
«2»	Менее 50%

МДК 03.02 Программно-аппаратные средства защиты информации

№	Вопрос	Уровень освоения	Осваиваемые профессиональные компетенции
1	**Происхождение термина «криптография»:** 1) от слова «тайнопись»; 2) от слова «шифрование»; 3) от термина «скремблирование»; 4) от термина «кодирование»;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
2	**Для чего используется система Kerberos?** 1) для симметричной аутентификации; 2) для несимметричной аутентификации; 3) для выработки ЭЦП; 4) для шифрования;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
3	**Наука об обеспечении секретности и / или аутентичности (подлинности) передаваемых сообщений:** 1) ЭЦП; 2) криптография; 3) криптоанализ; 4) стеганография;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**

4	**Системы, где с помощью открытого ключа шифруют ключ блочного криптоалгоритма, а само сообщение шифруют с помощью этого симметричного секретного ключа, называют:** 1) гибридные криптосистемы; 2) криптосистема RSA; 3) электронная подпись; 4) криптографические протоколы;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
5	**Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения:** 1) ключ; 2)разрядность блока; 3)число раундов шифрования; 4) алгоритм шифрования;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
6	**При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы называются:** 1) простыми криптосистемами; 2) гибридными криптосистемами; 3) ассиметричными криптосистемами; 4) симметричными криптосистемами;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
7	**Цифровая подпись - …** 1) подпись, которая ставится на документах; 2) небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа; 3) код с исправлением ошибок; 4) имитоприставка;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

8	**Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется:** 1) идентификацией; 2) аутентификацией; 3) авторизацией; 4) контролем целостности информации;	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
9	**Верификация – это** 1) это проверка принадлежности субъекту доступа предъявленного им идентификатора. 2) проверка целостности и подлинности информации, программы, документа 3) это присвоение имени субъекту или объекту	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
10	**Линейное шифрование – это** 1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу 2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому 3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**

11	**Подпись называется детерминированной, если** 1) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создается одна и та же подпись 2) для разных сообщений с использованием одного и того закрытого ключа при каждом подписывании создается одна и та же подпись 3) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создается одна и та же подпись	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
12	**Подпись называется рандомизированной, если** 1) для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи 2) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи 3) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
13	**Подпись, создаваемая DSS, является** 1) детерминированной 2) рандомизированной	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
14	**Подпись, создаваемая RSA, является** 1) детерминированной 2) рандомизированной	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**

15	**Последовательность случайных чисел должна быть** 1) монотонно возрастающей 2) монотонно убывающей 3) иметь равномерное распределение	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.**
16	**Алгоритм IDEA** 1) имеет переменную длину ключа 2) основан на сети Фейштеля 3) разбивает блок на фиксированные 16-битные подблоки	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
17	**Алгоритм ГОСТ 28147** 1) имеет переменную длину ключа 2) основан на сети Фейстеля 3) разбивает блок на фиксированные 16-битные подблоки	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
18	**Для создания подписи следует использовать** 1) свой открытый ключ 2) закрытый ключ получателя 3) свой закрытый ключ	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
19	**Под replay-атакой понимается:** 1) модификация передаваемого сообщения 2) повторное использование переданного ранее сообщения 3) невозможность получения сервиса законным пользователем	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

			ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.
20	**Атака «man in the middle» является** 1) пассивной 2) активной 3) может быть, как активной, так и пассивной	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
21	**Под DoS-атакой понимается:** 1) модификация передаваемого сообщения 2) повторное использование переданного ранее сообщения 3) невозможность получения сервиса законным пользователем	**2**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
22	**При односторонней аутентификации осуществляется аутентификация** 1) отправителя 2) получателя 3) KDC	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

23	**Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:** 1. черный пиар; 2. фишинг; 3. нигерийские письма; 4. источник слухов; 5. пустые письма.	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
24	**Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:** 1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов**
25	**Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:** 1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

26	**Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:** 1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
27	**Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:** 1. детектор; 2. доктор; 3. сканер; 4. ревизор; 5. сторож.	**1**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**
28	**Что такое несанкционированный доступ (нсд)?** 1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа 2) Создание резервных копий в организации 3) Правила и положения, выработанные в организации для обхода парольной защиты 4) Вход в систему без согласования с руководителем организации 5) Удаление не нужной информации	**2**	**ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.** **ПК 3.3. Фиксировать отказы в работе средств защиты.** **ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.**

29	**Методом Цезаря с использованием представленного алфавита и ключом 4 зашифровать слово ТЕСТО** 	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
30	**Методом Виженера с использованием представленного алфавита и ключом DOG зашифровать слово PROGRAM** 	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

<table>
<tr><td>31</td><td>Методом Плейера с использованием представленной таблицы и ключом TABLE зашифровать слово FOR EXAMPLE
 
</td><td>3</td><td>ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.</td></tr>
<tr><td>32</td><td>Методом Простой перестановки с использованием представленной таблицы зашифровать слово ЛЕВИТАЦИЯ
<table><tr><td>Л</td><td>И</td><td>Ц</td></tr><tr><td>Е</td><td>Т</td><td>И</td></tr><tr><td>В</td><td>А</td><td>Я</td></tr></table></td><td>3</td><td>ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.</td></tr>
</table>

33	**Методом Замены с использованием представленного алфавита и ключом зашифровать слово АЛГОРИТМ** 	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
34	**При помощи онлайн-сервиса CRYPT-ONLINE https://crypt-online.ru/ расшифруйте сообщение, зашифрованное алгоритмом RC4 0I/TmNOH0KbQo9On, используя в качестве ключа слово МЕЛ**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**
35	**При помощи онлайн-сервиса CRYPT-ONLINE https://crypt-online.ru/ расшифруйте сообщение, зашифрованное алгоритмом BASE64 0LvQvtC60L7QvQ==**	**3**	**ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.** **ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.**

Критерии оценивания:

Тестовое задание рассчитано на 45 мин.

Оценка	**Критерий**
«5»	80 – 100 % от общего числа баллов
«4»	70 - 75 %
«3»	50 - 65 %
«2»	Менее 50%

3.2. Промежуточная аттестация

Вопросы к дифференцированному зачету / экзамену по профессиональному модулю

МДК 03.01 Технические методы и средства, технологии защиты информации

Теоретические вопросы

1. Цели и задачи технической разведки
2. Принципы организации и ведения технической разведки
3. Оптическая разведка
4. Оптико-электронная разведка (ОЭР)
5. Радиоэлектронная разведка
6. Гидроакустическая разведка (ГАР)
7. Акустическая разведка (АР)
8. Радиационная разведка (РДР)
9. Химическая разведка (ХР)
10. Сейсмическая разведка (СР)
11. Магнитометрическая разведка (ММР)
12. Компьютерная разведка
13. Космическая разведка (КР)
14. Воздушная разведка (ВР)
15. Морская разведка (МР)
16. Наземная разведка (НР)
17. Обработка разведывательной информации
18. Основные показатели средств технической разведки
19. Вероятность обнаружения объектов
20. Вероятность распознавания объектов по параметрам принятых сигналов
21. Методики расчета вероятностей обнаружения и распознавания объектов
22. Дальность действия технических средств разведки
23. Оценка качества приема и воспроизведения перехваченной информации

24. Демаскирующие признаки объектов, влияющие на их обнаружение и распознавание

25. Технические характеристики радиоизлучений РЭСС

26. Групповые и индивидуальные технические демаскирующие признаки РЭСС

27. Оперативно-технические демаскирующие признаки РЭСС

28. Источники корабельных гидроакустических шумов

29. Гидроакустические сигналы

30. Маскирующие гидроакустические шумы

31. Затухание акустического поля

32. Каналы утечки информации через воздушную среду

33. Каналы утечки информации вибрационного типа

34. Каналы утечки информации электроакустического типа

35. Каналы утечки информации оптико-электронного типа

36. Каналы утечки информации параметрического типа

37. Каналы утечки информации при эксплуатации слаботочного оборудования

38. Каналы утечки информации при эксплуатации средств электронно-вычислительной техники и АСУ

37. Каналы перехвата информации при передаче ее по линиям связи

38. Цель, принципы и задачи защиты объектов от технической разведки

39. Общая классификация и характеристика способов защиты

40. Организационные мероприятия по защите информации в РЭС

41. Технические меры по защите информации в РЭС

42. Гидроакустическая маскировка НК и ПЛ

43. Маскировка сигналов гидроакустических средств

44. Пассивная защита объектов от акустической разведки

45. Активная защита объектов от акустической разведки

46. Организационные, организационно-технические и технические мероприятия защита информации при эксплуатации слаботочного оборудования

47. Поиск работающих технических средств разведки

48. Пассивные меры защиты информации

49. Создание помех средствам разведки

50. Криптографическая защита информации

51. Защита информации в средствах электронно-вычислительной техники от несанкционированного доступа

52. Защита информации в средствах электронно-вычислительной техники от технических средств разведки

53. Назначение и содержание технического контроля эффективности принимаемых мер защиты

54. Технические средства ЗИ при обращении пластиковых карт, виртуальной и реальной валюты.

Задачи (практические задания).

55. Проектирование объекта защиты.

56. Определение угроз защищаемой информации.

57. Проектирование комплекса организационных мероприятий по ЗИ.

58. Проектирование комплекса технических мероприятий по ЗИ.

59. Определение параметров защитных мер

60. Определение стоимости защитных мер и средств.

Практические задания для контроля и оценки результатов освоения ЗУН

1. Проектирование объекта защиты.

2. Определение угроз защищаемой информации.

3. Проектирование комплекса организационных мероприятий по ЗИ.

4. Проектирование комплекса технических мероприятий по ЗИ.

5. Определение параметров защитных мер

6. Определение стоимости защитных мер и средств.

МДК 03.02 Программно-аппаратные средства защиты информации

Теоретические вопросы

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примерыреализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности.

Показатели защищенности средств вычислительной техники от несанкционированного доступа.

13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
19. Биометрические средства идентификации и аутентификации пользователей.
20. Аутентификация субъектов в распределенных системах, проблемы ирешения. Схема Kerberos.
21. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
23. Законодательный уровень применения цифровой подписи.
24. Методы несимметричного шифрования. Использование

несимметричного шифрования для обеспечения целостности данных.

25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
26. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
27. Средства обеспечения информационной безопасности в ОС Windows’2000. Разграничение доступа к данным. Групповая политика.
28. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
29. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
30. Разграничение доступа к данным в ОС семейства UNIX.
31. Пользователи и группы в ОС UNIX.
32. Пользователи и группы в ОС Windows’2000.
33. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политикебезопасности.
34. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
35. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
36. Распределенные информационные системы. Удаленные

атаки на информационную систему.

37. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
38. Физические средства обеспечения информационной безопасности.
39. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
40. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
41. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
42. Виртуальные частные сети, их функции и назначение.

Практические задания

1. Анализ бизнес-требований к информационной безопасности
2. Разработка концептуального плана защиты.
3. Анализ технических ограничений плана защиты
4. Применение сертификатов для аутентификации и авторизации
5. Проектирование политики подачи заявок на сертификаты.
6. Проектирование размещения CRL и интервала публикации.
7. Проектирование защиты границ сети.
8. Зашита DNS. Проектирование политики IPSec.

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Основные источники:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMAR.
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
3. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

Дополнительные источники:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие. – СПб: НИУ ИТМО, 2018.
2. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации напредприятии. – СПб: Академия, 2018.
3. Хорев П.Б. методы и средства защиты информации в компьютерных системах. М.:Академия, 2018.

Интернет-ресурсы:

1. Единое окно доступа к образовательным ресурсам. Форма доступа: http://window.edu.ru.
2. Единая коллекция цифровых образовательных ресурсов. Форма доступа:http://schoolcollection. edu.ru.
3. http://www.mascom.ru/
4. http://nelk.ru/
5. http://www.laborkomplekt.ru/
6. http://pro-spec.ru/
7. http://www.bnti.ru
8. http://www.inside-zi.ru/