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

КОМПЛЕКТ КОНТРОЛЬНО ОЦЕНОЧНЫХ СРЕДСТВ

Профессионального модуля

ПМ01 Участие в планировании и организации работ по обеспечению защиты объекта

специальность
10.02.01 «Организация и технология защиты информации»

Нижний Новгород
2020 г.

Контрольно-оценочные средства профессионального модуля ПМ01 Участие в планировании и организации работ по обеспечению защиты объекта разработаны на основе ФГОС СПО по специальности: 10.02.01 Организация и технология защиты информации и рабочей программы профессионального модуля ПМ01 Участие в планировании и организации работ по обеспечению защиты объекта.

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

Комплект оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом профессионального модуля по специальности 10.02.01 «Организация и технология защиты информации».

В результате освоения профессионального модуля обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями**:**

уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности;
- использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
- проводить инструктаж персонала по организации работы с конфиденциальной информацией;
- контролировать соблюдение персоналом требований режима защиты информации;

знать:

- виды и способы охраны объекта;
- особенности охраны персонала организации;
- основные направления и методы организации режима и охраны объекта;
- разрешительную систему доступа к конфиденциальной информации;
- принципы действия аппаратуры систем контроля доступа;
- принципы построения и функционирования биометрических систем безопасности;
- требования и особенности оборудования режимных помещений;
- требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
- требования режима защиты информации при приеме в организации посетителей;
- организацию работы при осуществлении международного сотрудничества;
- требования режима защиты информации в процессе рекламной деятельности;
- требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
- задачи, функции и структуру подразделений защиты информации;
- принципы, методы и технологию управления подразделений защиты информации;

- методы проверки персонала по защите информации;
- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

иметь практический опыт:

- использования физических средств защиты объекта;
- применения физических средств контроля доступа на объект;
- ведения текущей работы исполнителей с конфиденциальной информацией;

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Участие в планировании и организации работ по обеспечению защиты объекта**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.1.	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации
ПК 1.2.	Участвовать в разработке программ и методик организации защиты информации на объекте
ПК 1.3.	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 1.4.	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности
ПК 1.5.	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации
ПК 1.6.	Обеспечивать технику безопасности при проведении организационно-технических мероприятий
ПК 1.7.	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите
ПК 1.8.	Проводить контроль соблюдения персоналом требований режима защиты информации
ПК 1.9.	Участвовать в оценке качества защиты объекта
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии в

	профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Применять математический аппарат для решения профессиональных задач
ОК 11.	Оценивать значимость документов, применяемых в профессиональной деятельности
ОК 12.	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность

Обучение по производственному модулю завершается экзаменом по профессиональному модулю.

2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Элемент модуля	Формы промежуточной аттестации	Форма предоставления отчетности
МДК 01.01. Обеспечение организации системы безопасности предприятия	Дифференцированный зачет	аттестационная ведомость
МДК 01.02. Организация работ подразделений защиты информации.	Дифференцированный зачет	аттестационная ведомость
МДК 01.03. Организация работы персонала с конфиденциальной информацией.	Экзамен	аттестационная ведомость
ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта	Экзамен по модулю	аттестационная ведомость

3. ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Текущий контроль

№	Вопрос	Уровень вопроса	Развивамые профессиональные компетенции
1	**Уязвимость информации — это:** А) Сведения об окружающем мире (объекте, процессе, явлении, событии), которые являются объектом преобразования (включая хранение, передачу и т. д.) и используются для выработки поведения, для принятия решения, для управления или для обучения Б) Это понятие, которое употребляется по отношению к отдельным лицам. Это есть право лица решать, какую информацию он желает разделить с другими, а какую хочет скрыть от других. В) Объективное свойство информации подвергаться различного рода воздействиям, нарушающим ее целостность, достоверность и конфиденциальность.	1	**ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
2	**Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?** А) Сотрудники Б). Хакеры В) Атакующие Г) Контрагенты (лица, работающие по договору)	1	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**

3	**Сотрудники группы режима (функции):** А) наблюдение за обстановкой вокруг объекта и на его территории; Б) определяют перечень сведений, составляющих коммерческую тайну, если таковые сведения не упомянуты в общегосударственных документах; В) разрабатывают положения и инструкции о порядке работы с конфиденциальной информацией и сведениями, составляющими тайну; Г) организуют и ведут закрытое делопроизводство, учет пользования, хранение и размножение документов и других, носителей конфиденциальной информации;	**2**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**
4	**Сотрудники группы охраны и сопровождения участвуют в:** А) в организации прохода персонала и посетителей в различные зоны безопасности; Б) в наблюдении за обстановкой вокруг объекта и на его территории; В) в экстренных действиях при возникновении угроз чрезвычайных обстоятельств; Г) осуществляют допуск персонала объекта к работе с конфиденциальной информацией, разрабатывают и осуществляют проверки выполнения сотрудниками объекта регламента работы с такой информацией;	**2**	**ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.** **ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации**
5	**Что из перечисленного не является целью проведения анализа рисков** А. Делегирование полномочий Б. Количественная оценка воздействия потенциальных угроз В. Выявление рисков Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер	**2**	**ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**

6	**Текущая работа с персоналом, обладающим конфиденциальной информацией, включает в себя:** А) Обучение и систематическое инструктирование сотрудников; Б) Проведение регулярной воспитательной работы. В)Постоянны контроль за выполнением персоналом требований по защите КИ. Г) Проведение служебных расследований пофакта утечки информации Д) Возможны все варианты.	**2**	**ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.** **ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**
7	**Что самое главное должно продумать руководство при классификации данных?** A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным B. Необходимый уровень доступности, целостности и конфиденциальности C. Оценить уровень риска и отменить контрмеры D. Управление доступом, которое должно защищать данные	**2**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**

8	**В качестве основных задач системы безопасности рассматриваются:** А) своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушению его нормального функционирования и развития; Б) создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия; В) пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности; Г) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей. Д) Возможны все варианты	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.**
9	**Доступ к конфиденциальным базам данных и файлам является:** А) Этаппом изготовления и издания конфиденциальных документов характеризующим наличие комплекса специальных документов Б) Этапом при использовании автоматизированной системы контроле в установленном графике. В) Завершающим этапом доступа сотрудника фирмы к компьютеру	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**

10	**Сохранение коммерческой тайны, борьба с хакерами – это** А) Физическая безопасность Б) Информационная безопасность В) Экологическая безопасность Г) Экономическая безопасность	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.**
11	**Защищенность информации означает:** А) невозможность несанкционированного использования или изменения; Б) независимость от чьего-либо мнения; В) удобство формы или обмена; Г) возможность получения данным потребителем.	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
12	**В соответствии с Федеральным законом от 8.08.2001 года №128–ФЗ деятельность различных подразделений службы безопасности предприятия подпадает под требования:** А) Заключать договор о неразглашении государственной тайны Б) Разрабатывать спецсредства для негласного получения информации В) Лицензировать свои виды деятельности Г) Предоставлять услуги в области шифрования	**3**	**ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**

13	**Анализ и прогноз динамики внешней и внутренней ситуации на предприятии, определение целей организационных структур службы безопасности, выявление проблем на пути достижения основной цели – это** А) Кадровое проектирование Б) Календарное управление В) Руководство Г) Стратегическое управление	**2**	**ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**
14	**Сотрудники этой группы участвуют в обеспечении безопасности деятельности объекта с помощью технических средств защиты** А) Детективная группа Б) Группа сопровождения В) Техническая группа Г) Группа безопасности	**1**	**ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**
15	**При организационном проектировании деятельности СБ предприятия первым этапом является:** А) Проектирование управленческой деятельности Б) Формулирование целей и задач системы управления В) Анализ и прогноз внешней ситуации Г) Расчет экономической эффективности Д) Решение основных вопросов формирования	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.**

16	**Эта специализированная группа разрабатывает и проводит специальные мероприятия по изучению отдельных лиц из числа персонала объекта, посетителей и клиентов фирмы и жителей ближайшего к объекту окружения, в действиях которых содержатся угрозы безопасности деятельности объекта.** А) Группа сектора охранной безопасности Б) Специализированная группа подбора В) Детективная группа Г) Группа внешних расследования	**1**	**ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите**
17	**Техническая группа:** А) Работает совместно с группой охраны Б) Отвечает за бесперебойную работу всех технических средств системы защиты объекта, ремонтирует и настраивает аппаратуру защиты В) проверяют кандидатов для приема на работу на объекте; Г) по отдельным заданиям руководства разрабатывают и проводят специальные мероприятия в отношении фирм-конкурентов;	**1**	**ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите**
18	**Что самое главное должно продумать руководство при классификации данных?** А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным Б Необходимый уровень доступности, целостности и конфиденциальности В Оценить уровень риска и отменить контрмеры Г Управление доступом, которое должно защищать данные	**1**	**ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**

19	**Безопасность информации – это** А) Совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также ее доступности для пользователей Б) Такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права; В) Такое ее состояние, при котором исключается возможность ее утечки за счет ПЭМИ и наводок, специальных устройств перехвата при передаче между объектами вычислительной техники Г) А и Б Д) Б и В	**1**	**ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
20	**Информационная безопасность РФ – это** А) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности и государства. Б) интересы государства создать условия для гармоничного развития, реализации конституционных прав и свобод человека и гражданина в конфиденциальности получения информации; В) интересы государства и прав человека в доступе информации, не запрещенной законом; защита информационных ресурсов от несанкционированного доступа	**1**	**ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
21	**Кто является основным ответственным за определение уровня классификации информации?** А. Руководитель среднего звена Б Высшее руководство В Владелец Г Пользователь	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на**

			объекте. **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
22	**Как называется информация, к которой ограничен доступ?** А) Конфиденциальная Б) Противозаконная В) Открытая Г) Недоступная	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.**
23	**Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это** А) уязвимость информации Б) надежность информации В) защищенность информации Г) безопасность информации	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**
24	**Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это** А) аудит Б) аутентификация В) авторизация Г) идентификация	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации** **ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности** **ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.**

25	**Основу политики безопасности составляет** А) программное обеспечение Б) управление рисками В) способ управления доступом Г) выбор каналов связи	**1**	**ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**
26	**Первым этапом разработки системы защиты ИС является** А) анализ потенциально возможных угроз Б) изучение информационных потоков В) стандартизация программного обеспечения Г) оценка возможных потерь	**1**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**

27	**Из перечисленного: 1) степень прогнозируемости; 2) природа происхождения; 3) предпосылки появления; 4) источники угроз; 5) размер ущерба — параметрами классификации угроз безопасности информации являются** А)1,5 Б)3,4,5 В)2,3,4 Г) 1,2,3	**2**	**ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.** **ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.** **ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.**
28	**На вашем компьютере хранится база данных о ваших коллегах: их персональные данные, электронные журналы и статьи. В последнее время вы заметили, что доступ к этой информации замедлился.** **Какое действие необходимо провести для устранения проблемы? Ответ пропишите** **_____**	**3**	**ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.** **ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.**
29	**Вы – сотрудник N- учреждения. Ежедневно в базе данных происходит накопление большого количества информации.** **Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.** **_____**	**3**	**ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.** **ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.**

30	**Гражданин П. проник в информационную базу ККБ и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.** **Являются ли его действия противозаконными?** **a) Да, ст.272** **b) Нет, недостаточно оснований для возбуждения дела**	**2**	**ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**
31	**По электронной почте Вам пришло сообщение, с прикрепленной к нему картинкой:**  **Содержит ли именно для Вас данное сообщение информацию?** **a) Да** **b) нет**	**3**	**ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.** **ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.** **ПК 1.9. Участвовать в оценке качества защиты объекта.**

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 01.01 Обеспечение организации системы безопасности предприятия

1. В каких направлениях производится оценка возможных угроз? Перечислите основные задачи системы защиты от возможных угроз и дайте характеристику средств защиты от возможных угроз.
2. Основные понятия безопасности предприятия.
3. Угрозы информационной безопасности на объекте. Модель угроз безопасности. Меры защиты.
4. Перечислите виды технических систем безопасности и дайте им характеристику.
5. Концептуальная модель информационной безопасности. План развития системы информационной безопасности.
6. Функциональные составляющие обеспечения безопасности предприятия
7. Уязвимые места в информационной безопасности. Несанкционированный доступ к источникам конфиденциальной информации.
8. Информационная безопасность автоматизированных информационных систем.
9. Направления обеспечения информационной безопасности. Организация режима и охраны.
10. Информационные системы: понятие, виды, классификация, назначение.
11. Угрозы информации: понятие, виды, классификация, назначение.
12. Концепция создания физической защиты важных объектов. Структура системы физической защиты. Концепция физической безопасности объекта.
13. Анализ уязвимости объекта. Цели и задачи анализа.
14. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
15. Методы и модели оценки уязвимости информации.
16. Организация службы экономической безопасности. Структура службы экономической безопасности. Предупредительная работа с персоналом.
17. Методы определения требований к защите информации.
18. Задачи службы безопасности. Организация внутри объектного режима.
19. Требования и рекомендации по защите информации. Причины потери информации. Основы организации защиты информации.
20. Оценки уязвимости информации.
21. Контрольно-пропускной режим на предприятии. Оборудование пропускных пунктов. КПП для прохода людей. Организация пропускного режима.
22. Методы определения требований к защите информации
23. Опасности и угрозы предприятию. Угрозы безопасности информации и их классификация.
24. Объясните состав и структуру службы безопасности.

25. Объясните информационную безопасность предприятия и обеспечение организационной защиты.
26. Архитектура систем защиты информации.
27. Объясните основные принципы организационной защиты информации.
28. Что такое политика безопасности предприятия и опишите, что она в себя включает.
29. Объясните, что такое государственная тайна и как осуществляется допуск к сведениям, составляющим государственную тайну. Ответственность за нарушение государственной тайны.
30. Организация пропускного режима и пропускные документы.
31. Объясните, что такое коммерческая тайна и как осуществляется допуск к сведениям, составляющим коммерческую тайну.
32. Основные задачи обеспечения защиты информации, циркулирующей в автоматизированной информационной системе.
33. Объясните действия руководства и службы безопасности по обеспечению безопасности предприятия.
34. Объясните организацию пропускного режима и пропускные документы.
35. Объясните концептуальную модель безопасности продукции и концептуальную модель безопасности информации.
36. Объясните степени секретности сведений и грифы секретностей носителей этих сведений.
37. В чем особенность порядка учета, хранения и обращения с документами и изделиями с грифом «Коммерческая тайна» на предприятии.
38. Что включает в себя политика информационной безопасности предприятия?
39. В чем заключаются особенности и основные требования защиты персональных данных в автоматизированных информационных системах? Объясните категории обрабатываемых в информационной сфере персональных данных.
40. В чем особенность режимно-секретных органов, постоянно действующих технических комиссий и их полномочий?
41. Служба безопасности предприятия и ее общие функции, задачи. Объясните организационную структуру службы безопасности предприятия.
42. Что включает в себя технология управления информационной безопасностью?
43. Классификация угроз безопасности информации. Какие формы утечки информации существуют?
44. Объясните основные организационно-технические мероприятия по защите информации.
45. Объясните несанкционированный доступ к источникам конфиденциальной информации.
46. Перехват информации и как он осуществляется.
47. Объясните структуру организационного обеспечения безопасности предприятия.

48. Назовите и объясните основные составляющие информационной безопасности.
49. Назовите и объясните причины потери информации и основы организации защиты информации.
50. Принципы, цели и задачи системы обеспечения безопасности объекта.

МДК 01.02 Организация работ подразделений защиты информации

1. Задачи, функции, организационная структура подразделения защиты информации
2. Нормативная база организации работы подразделения защиты информации (виды, назначение, краткое содержание документов)
3. Процедура установления режима коммерческой тайны на предприятии
4. Разрешительная система доступа к конфиденциальной информации
5. Функции процессов управления подразделением защиты информации
6. Методы управления подразделением защиты информации
7. Основы кадровой безопасности
8. Особенности трудовых отношений при работе с конфиденциальной информацией
9. Подбор и расстановка кадров в подразделении защиты информации
10.Профессиональный рост персонала подразделения защиты информации
11. Управление лояльностью персонала подразделения защиты информации
12. Управление ПЗИ в кризисных ситуациях 13.Инструктаж персонала по защите информации 14.Обучение, сертификация персонала, имеющего доступ к конфиденциальной информации
15. Контроль соблюдения персоналом требований режима защиты информации
16. Организация проверки персонала по защите информации 17.Работа с персоналом при увольнении сотрудника 18.Проведение служебного расследования 19.Противодействие инсайдерской информации
20.Взаимодействие сотрудников ПЗИ с правоохранительными органами
21.Взаимодействие сотрудников ПЗИ с органами государственного управления, контроля и надзора
22. Деятельность подразделений защиты информации по проверке контрагентов
23. Конкурентная разведка 24.Противодействие социальной инженерии
25.Использование системы корпоративной безопасности для отражения рейдерской атаки

МДК 01.03. Организация работы персонала с конфиденциальной информацией

1. Понятия «служба безопасности», «секретный отдел», «первый отдел», «особый отдел» в исторических аспектах развития.

2. Структура и основные задачи секретного отдела.
3. Организация работы секретного отдела.
4. Функции режимно-секретного подразделения.
5. Методы работы с персоналом, имеющим доступ к КИ: возможные причины разглашения КИ.
6. Методы работы с персоналом, имеющим доступ к КИ: основные этапы и направления работы с персоналом.
7. Методы работы с персоналом, имеющим доступ к КИ: технология подбора кандидатов на вакантные должности.
8. Методы работы с персоналом, имеющим доступ к КИ: основные требования к кандидатам на вакантные должности.
9. Методы работы с персоналом, имеющим доступ к КИ: Инструкция о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне.
10. Методы работы с персоналом, имеющим доступ к КИ: задачи, формы и методы обучения персонала.
11. Методы работы с персоналом, имеющим доступ к КИ: контроль качества работы персонала.
12. Методы работы с персоналом, имеющим доступ к КИ: процедура увольнения сотрудника.
13. Разработка разрешительной системы доступа к КИ.
14. Мотивация деятельности персонала секретного отдела.
15. Разработка должностной инструкции работника секретного отдела.
16. Организация работы сотрудника секретного отдела.
17. Подготовка совещаний конфиденциального характера.
18. Организация доступа участников при проведении конфиденциальных совещаний.
19. Оформление протокола конфиденциального совещания. Использование материалов по итогам совещания.
20. Требования к участникам конфиденциального совещания.
21. Организация защиты информации при осуществлении рекламной деятельности.
22. Организация защиты информации при осуществлении публикационной деятельности.
23. Обязанности и права экспертной комиссии при подготовке публикаций.
24. Организация защиты информации при осуществлении выставочной деятельности.
25. Организация защиты информации при взаимодействии со СМИ.
26. Основные направления международного сотрудничества в области обеспечения информационной безопасности.
27. Процедура создания носителя конфиденциальной информации.
28. Оформление бумажных носителей конфиденциальной информации.
29. Организация хранения носителей конфиденциальной информации.
30. Условия хранения носителей конфиденциальной информации.
31. Передача носителей конфиденциальной информации.

32. Особенности доступа к информации, содержащей персональные данные.
33. Особенности доступа к архивным конфиденциальным документам.
34. Цель и задачи внутреннего расследования по фактам утраты (разглашения) КИ.
35. Состав, права и обязанности комиссии по расследованию фактов утраты (разглашения) КИ.
36. Документирование результатов расследования фактов утраты (разглашения) КИ.

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОБУЧЕНИЯ

Основные источники:

1. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.
2. Хачатрян, Г. А. Организация и технология работы с конфиденциальными документами : учебник для СПО / Г. А. Хачатрян, И. В. Кузнецова. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2020. — 283 с. — ISBN 978-5-4488-0742-8, 978-5-4497-0783-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.

Дополнительные источники:

отсутствуют

Интернет-ресурсы:

Федеральный портал «Российское образование» - http: //www. edu.ru/