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

# Комплект контрольно-оценочных средств

по

## ПП.03 Производственная практика

для специальности

## 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2021

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

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

## СОДЕРЖАНИЕ

## 1. Паспорт комплекта оценочных средств

### 1.1 Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по ПП.03 Производственная практика, которые соотнесены с требуемыми результатами освоения образовательной программы (компетенциями выпускников). Совокупность запланированных результатов обучения должна обеспечивать выпускнику освоение всех общих компетенций (далее – ОК), профессиональных компетенций (далее – ПК), установленных ФГОС СПО.

Контрольно-оценочные средства (далее - КОС) предназначены для контроля и оценки образовательных достижений обучающихся по ПП.03 Производственная практика.

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

КОС разработан на основании рабочей программы ПП.03 Производственная практика.

**1.2 Планируемые результаты освоения** ПП.03 Производственная практика**:**

В результате освоения ПП.03 Производственная практика обучающийся должен **уметь**:

**уметь**:

- У1 применять технические средства для криптографической защиты информации конфиденциального характера;
- У2 применять технические средства для уничтожения информации и носителей информации;
- У3 применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- У4 применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- У5 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- У6 применять инженерно-технические средства физической защиты объектов информатизации.

В результате освоения ПП.03 Производственная практика обучающийся должен **знать**:

- З1 порядок технического обслуживания технических средств защиты информации;

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

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

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

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

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

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

− З8 основные способы физической защиты объектов информатизации;

− З9 номенклатуру применяемых средств физической защиты объектов информатизации.

В результате освоения ПП.03 Производственная практика обучающийся должен **иметь практический опыт:**

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

− ПО2 технического обслуживания технических средств защиты информации;

− ПО3 применения основных типов технических средств защиты информации;

− ПО4 выявления технических каналов утечки информации;

− ПО5 участия в мониторинге эффективности технических средств защиты информации;

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

− ПО7 проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при

аттестации объектов информатизации по требованиям безопасности информации;

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

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

**Профессиональные и общие компетенции**, которые формируются при прохождении ПП.03 Производственная практика:

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

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

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

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

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

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а

также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

**Планируемые личностные результаты освоения рабочей программы ПП.03 Производственная практик:**

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

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

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

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

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

## 1.3 Контроль и оценка результатов освоения ПП.03 Производственная практика

**Таблица 1**

| Код и наименование профессиональных и общих компетенций, формируемые в рамках производственной практики | Критерии оценки | Методы оценки |
|---|---|---|
| ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации | Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной | Оценка процесса и результатов выполнения видов работ на практике |

| | | |
|---|---|---|
| | документации | |
| ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации | Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации | Оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа | Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа | Оценка процесса и результатов выполнения видов работ на практике |
| ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. | Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении | Оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации | Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации | Оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации | Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации | Оценка процесса и результатов выполнения видов работ на практике |

## 2. Оценочные материалы для проведения текущего контроля успеваемости обучающихся по ПП.03 Производственная практика

Контроль качества освоения производственной практики включает в себя текущий контроль успеваемости, который проводится в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования общих и профессиональных компетенций. Текущий контроль проводится при оценке процесса и результатов выполнения видов работ на практике.

### 2.1. Виды работ на практике.

1. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

2. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

3. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

4. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

**Критерии оценивания выполненных заданий по видам работ на практике**

| Оценка | Критерии оценивания |
|---|---|
| 5 (отлично) | Практические задания по видам работ выполнены в полном объеме, обучающийся применил все знания, полученные ранее при теоретическом обучении, закрепил знания в процессе практики. В ходе устного опроса обучающийся демонстрирует системность и глубину знаний, полученных при прохождении практики, соответствующих |

| | |
|---|---|
| | содержанию программы практики: дает исчерпывающие ответы на вопросы преподавателя по темам, предусмотренным программой практики; может аргументированно сделать выводы и сформулировать свое мнение; владеет нормами литературного языка, терминологией; грамотно, стилистически верно, логически правильно излагает ответы на вопросы; правильно и логически последовательно выполняет задания, предусмотренные программой практики. |
| 4 (хорошо) | Практические задания выполнены в полном объеме, обучающийся применил знания, полученные ранее при теоретическом обучении, закрепил знания в процессе практики, но были выявлены 2-3 ошибки при выполнении практических заданий. В процессе устного опроса обучающийся демонстрирует достаточную полноту знаний в объеме программы практики, при наличии 1–2 несущественных ошибки в изложении ответов: допускает незначительные ошибки, но исправляется при наводящих вопросах преподавателя; делает выводы, но они требуют дополнительной аргументации; владеет нормами литературного языка, необходимой для ответа терминологией; правильно выполняет задания, предусмотренные программой практики, но допускает непоследовательность при их выполнении. |
| 3 (удовлетворительно) | Практические задания выполнены в полном объеме, обучающийся поверхностно применил знания, полученные ранее при теоретическом обучении, допустил несколько существенных ошибок при выполнении практических заданий, имеются замечания по их оформлению. В процессе устного опроса обучающийся демонстрирует недостаточные знания по вопросам программы практики; использует специальную терминологию, но допускает 1–2 ошибки в определении основных понятий, затрудняется исправить ошибки самостоятельно; делает выводы, но не может привести научную аргументацию; способен самостоятельно, но поверхностно анализировать материал, раскрывает сущность решаемой проблемы только при наводящих вопросах преподавателя; правильно применяет методы при |

| | |
|---|---|
| | выполнении заданий, предусмотренных программой практики, но выполненные задания содержат ошибки. |
| 2 (удовлетворительно) | Практические задания выполнены частично, обучающийся допустил многочисленные ошибки при их выполнении, имеются многочисленные замечания по оформлению практических заданий. В ходе устного опроса обучающийся демонстрирует фрагментарные знания в рамках программы практики; не владеет минимально необходимой терминологией; допускает грубые логические ошибки, отвечая на вопросы преподавателя, которые не может исправить самостоятельно; не может выполнить полученные на защите отчета задания. |

## 3. Оценочные материалы для организации промежуточной аттестации по ПП.03 Производственная практика в форме дифференцированного зачета

Показатели оценивания компетенций, формируемых в результате прохождения практики, складываются из:

– показателей оценивания практических заданий;

– показателей оценивания отчета по практике;

– показателей защиты отчета по практике, отражающие способность обучающегося защищать результаты своей работы в части сформированности компетенций, предусмотренных программой практики.

### 3.1. Перечень вопросов по видам работ на практике для защиты отчета.

1. 1. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.

Вопросы:

1.Как провести обследование деятельности предприятия? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

2.Как проводить инструкцию по охране труда и технике безопасности на предприятии? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

3.Как выполнить исследование угроз и методологии оценки уязвимости информации информационных рисков? (оцениваемые знания, умения,

компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

4. Какой определить подход к исследованию методов и разработки моделей оценки уязвимости информации? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

5. Как определить методы по исследованию и разработке аналитических моделей для определения базовых показателей уязвимости информации? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

6. Участие в проектировании политики безопасности информационного объекта. (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

7. Как спроектировать политику безопасности информационного объекта на конкретном пример? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

8. Как разработать мероприятия по выявлению каналов утечки информации (специальные обследования)? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

2. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.

Вопросы:

1. Как разработать план по участию в разработке проекта монтажа технических средств защиты информации в телефонных линиях? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

2. Как разработать план по участию в обслуживании и эксплуатации технических средств защиты информации в телефонных линиях? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9,

У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

3.Определите оценку эффективности защиты речевой информации. (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

4. Как рассчитать инструментально-расчётную оценку защищённости защищаемого помещения от утечки речевой информации? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

5. Как разработать план по участию в разработке проекта монтажа, обслуживания и эксплуатации средств охраны и безопасности: датчики движения для охраны помещений? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

3. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

Вопросы:

1. Как разработать план по участию в разработке проекта монтажа, обслуживания и эксплуатации средств инженерной защиты и технической охраны объектов: системы защиты от утечки информации по оптическому каналу? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5).

2. Как выполнить проектирование системы видеонаблюдения за протяженным периметром? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

3. Как выполнить проектирование системы идентификации людей на входе в здание? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

4. Как выполнить проектирование системы видеонаблюдения в транспорте. Проектирование системы видеонаблюдения в организации? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9,

У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

5. Как определить участие в разработке проекта монтажа систем видеонаблюдения, его обслуживании и эксплуатации? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

4. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

Вопросы:

1. Как разработать план по участию в разработке проекта монтажа, обслуживания и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по акустическому каналу пассивными методами? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

2. Как разработать план по участию в разработке проекта монтажа, обслуживания и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: системы защиты от утечки информации по электросетевому каналу? (оцениваемые знания, умения, компетенции: З 1, З2, З3, З4, З5, З6, З7, З8, З9, У1, У2, У3, У4, У5, У6, ОК.01-ОК10, ПО 1, ПО2, ПО3, ПО4, ПО5, ПО6 , ПО7, ПО8, ПО9, ПК. 3.1, ПК 3.2, ПК.3.3, ПК3.4, ПК.3.5)

**Критерии оценивания**

| Оценка | Критерии оценивания |
|---|---|
| 5 (отлично) | Практические задания выполнены в полном объеме, обучающийся применил все знания, полученные ранее при теоретическом обучении и необходимые для их выполнения, закрепил знания в процессе практики. Содержание отчета по практике: отчет собран в полном объеме; структурированность; не нарушены сроки сдачи отчета. На защите отчета обучающийся демонстрирует системность и глубину знаний, полученных при прохождении практики, соответствующих содержанию программы практики: дает исчерпывающие ответы на вопросы преподавателя по темам, |

| | |
|---|---|
| | предусмотренным программой практики; может аргументированно сделать выводы и сформулировать свое мнение; владеет нормами литературного языка, терминологией; грамотно, стилистически верно, логически правильно излагает ответы на вопросы; правильно и логически последовательно выполняет задания, предусмотренные программой практики. |
| 4 (хорошо) | Практические задания выполнены в полном объеме, обучающийся применил знания, полученные ранее при теоретическом обучении и необходимые для их выполнения, закрепил знания в процессе практики, но были выявлены 2-3 ошибки при выполнении практических заданий. Содержание отчета по практике: отчет собран в полном объеме; не везде прослеживается структурированность; не нарушены сроки сдачи отчета. На защите отчета обучающийся демонстрирует достаточную полноту знаний в объеме программы практики, при наличии 1–2 несущественных ошибки в изложении ответов: допускает незначительные ошибки, но исправляется при наводящих вопросах преподавателя; делает выводы, но они требуют дополнительной аргументации; владеет нормами литературного языка, необходимой для ответа терминологией; правильно выполняет задания, предусмотренные программой практики, но допускает непоследовательность при их выполнении. |
| 3 (удовлетворительно) | Практические задания выполнены в полном объеме, обучающийся поверхностно применил знания, полученные ранее при теоретическом обучении и необходимые для их выполнения, допустил несколько существенных ошибок при выполнении практических заданий, имеются замечания по их оформлению. Содержание отчета по практике: отчет собран в полном объеме; не везде прослеживается структурированность; в оформлении отчета прослеживается небрежность. На защите отчета обучающийся демонстрирует недостаточные знания по вопросам программы практики; использует специальную терминологию, но допускает 1–2 ошибки в определении основных понятий, затрудняется исправить ошибки самостоятельно; делает выводы, но не может привести научную аргументацию; способен |

| | |
|---|---|
| | самостоятельно, но поверхностно анализировать материал, раскрывает сущность решаемой проблемы только при наводящих вопросах преподавателя; правильно применяет методы при выполнении заданий, предусмотренных программой практики, но выполненные задания содержат ошибки. |
| 2 (удовлетворительно) | Практические задания выполнены частично, допустил многочисленные ошибки при их выполнении, имеются многочисленные замечания по оформлению практических заданий. Содержание отчета по практике: отчет собран не в полном объеме; нарушена структурированность; в оформлении отчета прослеживается небрежность; нарушены сроки сдачи отчета. На защите отчета обучающийся демонстрирует фрагментарные знания в рамках программы практики; не владеет минимально необходимой терминологией; допускает грубые логические ошибки, отвечая на вопросы преподавателя, которые не может исправить самостоятельно; не может выполнить полученные на защите отчета задания. |

## 4. Информационное обеспечение

**Основные источники:**


1. Технические средства информатизации. Учебник для СПО/ Е. И. Гребенюк, Н. А. Гребенюк М.: ИЦ Академия,2019 – 352 с.
2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А.,М.: ИЦ Академия, 2019 – 272 с.


**Дополнительные источники:**


1. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012
2. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
3. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.
5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013 – 172 с.
6. Организационно-правовое обеспечение Информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов,В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с
7. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии

с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
21. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
22. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
24. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
25. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
26. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
27. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
28. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

29. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
30. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
31. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
32. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
34. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
35. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
36. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
37. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
38. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
39. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
40. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
41. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

42. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
43. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
46. Номенклатура показателей качества. Ростехрегулирование, 2005.
47. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
48. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
49. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
50. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
51. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
53. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
54. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

55. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
56. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
57. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
58. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
59. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

**Электронные издания (электронные ресурсы):**

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548
3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. https://urait.ru/bcode/451933
4. Интерфейсы периферийных устройств – https://intuit.ru/studies/courses/92/92/lecture/28396
5. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2
6. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146
7. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074
8. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240

9. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158
10. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157

**Цифровая образовательная среда СПО PROFобразование**:

- Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 c. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87882 (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

**Электронно-библиотечная система:**

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

**Веб-система для организации дистанционного обучения и управления им:**

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