

**Приложение ППСЗ по специальности 10.02.05 Обеспечение информационной
безопасности автоматизированных систем 2021-2022 уч.г.:
Комплект контрольно-оценочных средств УП.02 Учебная практика**

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

**Комплект
контрольно-оценочных средств**

по

УП.02 Учебная практика

**для специальности
10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

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:

Ляшенко А.В., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств
 - 1.1 Область применения комплекта оценочных средств
 - 1.2 Планируемые результаты освоения УП.02 Учебная практика:
 - 1.3 Контроль и оценка результатов освоения УП.02 Учебная практика
2. Оценочные материалы для проведения текущего контроля успеваемости обучающихся по УП.02 Учебная практика
3. Оценочные материалы для организации промежуточной аттестации по УП.02 Учебная практика в форме дифференцированного зачета
4. Информационное обеспечение

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 УП.02 Учебная 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 УП.02 Учебная 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 УП.02 Учебная практика.

1.2 Планируемые результаты освоения УП.02 Учебная практика:

В результате освоения УП.02 Учебная практика обучающийся должен **уметь**:

- У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- У.2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных;
- У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- У.6 применять математический аппарат для выполнения криптографических преобразований;
- У.7 использовать типовые программные криптографические средства, в том числе электронную подпись;
- У.8 применять средства гарантированного уничтожения

информации;

- У.9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

- У.10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения УП.02 Учебная практика обучающийся должен **знать:**

- 3.1особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

- 3.2методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

- 3.3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

- 3.4основные понятия криптографии и типовых криптографических методов и средств защиты информации;

- 3.5особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

- 3.6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

В результате освоения УП.02 Учебная практика обучающийся должен **иметь практический опыт:**

- ПО1 установки, настройки программных средств защиты информации в автоматизированной системе;

- ПО2 обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

- ПО3 тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

- ПО4 решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

- ПО5 применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

- ПО6 учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

- П7 работы с подсистемами регистрации событий;

- ПО8 выявления событий и инцидентов безопасности в автоматизированной системе.

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

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

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

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие

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

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

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

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

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

ОК 09 Использовать информационные технологии в профессиональной деятельности

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Планируемые личностные результаты освоения рабочей программы УП.02 Учебная практика:

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично 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 УП.02 Учебная практика

Таблица 1

Код и наименование профессиональных и общих компетенций, формируемые в учебной практики	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	Оценка процесса и результатов выполнения видов работ на практике

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	Оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	Оценка процесса и результатов выполнения видов работ на практике
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Оценка процесса и результатов выполнения видов работ на практике

2. Оценочные материалы для проведения текущего контроля успеваемости обучающихся по УП.02 Учебная практика

Контроль качества освоения учебной 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 программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах (оцениваемые знания, умения, компетенции: З 1, У 1, У2, ОК1-10, ПО 2, ПК. 2.2, ПК 2.1, ПК.2.3)

2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З 2, У 3, У4, ОК1-10, ПО 3, ПК. 2.2, ПК.2.3)

3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З 2, З6, У 4, У 5, У10, ОК1-10, ПО 4, ПК. 2.2. ПК 2.3, ПК.2.6)

4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации (оцениваемые знания, умения, компетенции: З 1, З 2, З3, З6, У 5, У10, , ОК1-10, ПО 6, ПК. 2.3, ПК.2.6)

5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации (оцениваемые знания, умения, компетенции: З 1, З 2, З3, З6, У 4, У5, У7 ,У10, ОК1-10, ПО 6, ПК. 2.4. 2.5.)

6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. (оцениваемые знания, умения, компетенции: З3, З6, У 3,У 4, У5, У8, ОК1-10, ПО 4, ПО5, ПО7, ПК. 2.6, ПК.2,3)

7. Устранение замечаний по результатам проверки (оцениваемые знания, умения, компетенции: З 1, З5, У3, У 8, ОК1-10, ПО4, ПО 8, ПК. 2.3, ПК.2.6)

8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. (оцениваемые знания, умения, компетенции: З 1, З6, У3, У9,У 4, ОК1-10, ПО 3, ПО4, ПО8, ПК. 2.3, ПК.2,6)

9. Применение математических методов для оценки качества и выбора наилучшего программного средства (оцениваемые знания, умения, компетенции: З4, З6, У6, ОК1-10, ПО 5, ПК. 2.2, ПК.2,4)

10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи (оцениваемые знания, умения, компетенции: З4, З6, У 7, ОК1-10, ПО 5, ПК. 2.2, ПК.2,4)

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 УП.02 Учебная 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. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах (оцениваемые знания, умения, компетенции: З 1, У 1, У2, ОК1-10, ПО 2, ПК. 2.2, ПК 2.1, ПК.2.3)

Вопросы:

1. Какие основные категории программных средств используются для обеспечения информационной безопасности в автоматизированных системах?
2. Чем отличаются программные и программно-аппаратные средства обеспечения информационной безопасности?
3. Какие аппаратные средства используются для повышения уровня информационной безопасности в автоматизированных системах?

2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З 2, У 3, У4, ОК1-10, ПО 3, ПК. 2.2, ПК.2.3).

Вопросы:

1. Какие методы диагностики используются для выявления неисправностей в программно-аппаратных средствах обеспечения информационной безопасности?
2. Какие этапы включает процесс устранения отказов в работе программно-аппаратных средств ИБ?
3. Какие подходы применяются для мониторинга состояния и исправления ошибок в шифрующих устройствах?

3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З 2, З6, У 4, У 5, У10, ОК1-10, ПО 4, ПК. 2.2. ПК 2.3, ПК.2.6).

Вопросы:

1. Какие критерии используются для оценки эффективности программно-аппаратных средств обеспечения информационной безопасности?
2. Какие показатели отражают уровень защиты данных при использовании шифрования?
3. Какие факторы влияют на общую оценку эффективности комплексных программно-аппаратных решений по обеспечению информационной безопасности?

4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации (оцениваемые знания, умения, компетенции: З 1, З 2, З3, З6, У 5, У10, , ОК1-10, ПО 6, ПК. 2.3, ПК.2.6).

Вопросы:

1. Какие разделы должна включать документация по учету конфиденциальной информации?
2. Какие процессы и операции включаются в документацию по обработке конфиденциальной информации?
3. Какие меры безопасности необходимо предусмотреть при разработке процедур хранения конфиденциальной информации?
4. Какие способы передачи конфиденциальной информации являются наиболее надежными и безопасными?

5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации (оцениваемые знания, умения, компетенции: З 1, З 2, З3, З6, У 4, У5, У7 ,У10, ОК1-10, ПО 6, ПК. 2.4. 2.5.).

Вопросы:

1. Какие виды программного обеспечения используются для обработки конфиденциальной информации?
2. Какие функции должно иметь программное обеспечение для надежного хранения конфиденциальной информации?
3. Какие алгоритмы шифрования используются в программном обеспечении для защиты конфиденциальной информации?

4. Какие требования предъявляются к программному обеспечению для передачи конфиденциальной информации?
5. Какие стандарты безопасности должны соблюдаться при выборе программного обеспечения для работы с конфиденциальной информацией?

6. Составление маршрута и состава проведения различных **видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.** (оцениваемые знания, умения, компетенции: ЗЗ, З6, УЗ, У4, У5, У8, ОК1-10, ПО4, ПО5, ПО7, ПК. 2.6, ПК.2,3).

Вопросы:

1. Какие этапы включает процесс составления маршрута проведения контрольных проверок при аттестации объектов?
2. Какие виды контрольных проверок проводятся при аттестации объектов информатизации?
3. Какие специалисты привлекаются к проведению контрольных проверок при аттестации объектов?
4. Какие документы оформляются в ходе подготовки к контрольным проверкам при аттестации объектов?
5. Какие критерии оцениваются при проведении контрольных проверок помещений?

7. Устранение замечаний по результатам проверки (оцениваемые знания, умения, компетенции: З1, З5, УЗ, У8, ОК1-10, ПО4, ПО8, ПК. 2.3, ПК.2.6).

Вопросы:

1. Какие основные категории замечаний могут быть выявлены в результате проверки?
2. Какие шаги необходимо предпринять для устранения замечаний, связанных с документацией?
3. Какие меры следует принять для устранения технических замечаний, выявленных в ходе проверки?
4. Какие действия требуются для устранения замечаний, касающихся соблюдения нормативных требований?

8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. (оцениваемые знания, умения, компетенции: З1, З6, УЗ, У9, У4, ОК1-10, ПОЗ, ПО4, ПО8, ПК. 2.3, ПК.2,6).

Вопросы:

1. Какие законодательные акты и нормативные документы служат основой для разработки нормативных методических документов по обеспечению информационной безопасности?
2. Какие программно-аппаратные средства рассматриваются в нормативных документах по обеспечению информационной безопасности?

3. Какие критерии используются для оценки эффективности применения программно-аппаратных средств в области информационной безопасности?
4. Какие методы и подходы используются для анализа текущего состояния информационной безопасности в организации?

9. Применение математических методов для оценки качества и выбора наилучшего программного средства (оцениваемые знания, умения, компетенции: 34, 36, У6, ОК1-10, ПО 5, ПК. 2.2, ПК.2,4)

Вопросы:

1. Какие математические методы используются для оценки качества программного обеспечения?
2. Какие критерии оценки качества программного продукта можно выделить?
3. Какие статистические методы применяются для сравнения различных программных средств?

10. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи (оцениваемые знания, умения, компетенции: 34, 36, У 7, ОК1-10, ПО 5, ПК. 2.2, ПК.2,4)

Вопросы:

1. Какие основные криптографические алгоритмы используются для защиты информации?
2. Какие типовые криптографические средства применяются для шифрования данных?
3. Какие преимущества и недостатки имеет симметричное шифрование по сравнению с асимметричным?
4. Какие методы аутентификации применяются вместе с электронными подписями?

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. Ильин, М. Е., Калинкина, Т. И., Пржегорлинский, В. Н., Криптографическая защита информации в объектах информационной инфраструктуры: учебник, 1-е изд.,/ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с.

2. 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.

Дополнительные источники:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. – М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. - М.: МЦНМО, 2006.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. 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».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
11. 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.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. 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.
14. 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.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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 недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи в ограниченном доступе, не содержащих сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. 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

24. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

25. 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

26. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

27. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

28. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

29. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

30. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

31. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

32. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
34. 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.
35. 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.
36. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
37. 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.
38. 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.
39. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
40. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
41. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
42. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
45. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
46. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Электронные издания (электронные ресурсы):

1. Адаменко, М.В. Основы классической криптографии: секреты шифров и кодов / М.В. Адаменко/ – 2-е изд., испр. И доп. – Москва: ДМК Пресс, 2016. – 296 <https://e.lanbook.com/book/82817>

2. 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>

3. 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>

4. 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>

Цифровая образовательная среда СПО PROФобразование:

Пацинская, Л. И. Социально-экономические аспекты современного общества : учебное пособие / Л. И. Пацинская. — Воронеж : Воронежский государственный университет инженерных технологий, 2018. — 208 с. — ISBN 978-5-00032-379-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование : [сайт]. — URL: <https://profspo.ru/books/88435> (дата обращения: 12.07.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPRBOOKS - <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/>