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

Комплект контрольно-оценочных средств

по

ПП.02 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:
Ляшенко А.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.02 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.02 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.02 Производственная практика.

1.2 Планируемые результаты освоения ПП.02 Производственная практика**:**

В результате освоения ПП.02 Производственная 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 - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения ПП.02 Производственная практика обучающийся должен **знать**:

З 1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З 2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З 3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З 4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З 5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З 6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

В результате освоения ПП.02 Производственная практика обучающийся должен **иметь практический опыт:**

ПО 1 - установки, настройки программных средств защиты информации в автоматизированной системе;

ПО 2 - обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

ПО 3 - тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

ПО 4 - решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

ПО 5 - применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

ПО 6 - учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

ПО 7 - работы с подсистемами регистрации событий;

ПО 8 - выявления событий и инцидентов безопасности в автоматизированной системе.

Профессиональные и общие компетенции, которые формируются при прохождении ПП.02 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 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 ПП.02 Производственная практика :

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.02 Производственная практика

Таблица 1

Код и наименование профессиональных и общих компетенций, формируемые в рамках междисциплинарного курса	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 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 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 защите автоматизированных (информационных) систем С использованием программных и программно-аппаратных средств предупреждения обнаружения, и ликвидации последствий компьютерных атак	оценка процесса и результатов выполнения видов работ на практике

2. Оценочные материалы для проведения текущего контроля успеваемости обучающихся по ПП.02 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. Анализ принципов построения систем информационной защиты производственных подразделений (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)
2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

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 (неудовлетворительно)	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.02 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. Анализ принципов построения систем информационной защиты производственных подразделений (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие основные принципы лежат в основе построения систем информационной защиты производственных подразделений?
2) Как классифицируются угрозы информационной безопасности в производственных подразделениях?

3) Какие нормативные документы регулируют защиту информации в автоматизированных системах на производстве?
4) Какие методы и средства используются для защиты информации от несанкционированного доступа в производственных подразделениях?
5) Какова роль программно-аппаратных средств в обеспечении информационной безопасности на производстве?
6) Какие этапы включает процесс построения системы информационной защиты производственного подразделения?
7) Какие виды атак наиболее характерны для автоматизированных систем производственных подразделений?
8) Как осуществляется контроль целостности данных в системах информационной защиты?
9) Какие методы шифрования данных применяются в производственных подразделениях?
10) Как организовать защиту информации на уровне сетевого взаимодействия в производственных подразделениях?
11) Какие программные средства используются для обнаружения и предотвращения вторжений в автоматизированных системах?
12) Как обеспечить безопасность данных при передаче между производственными подразделениями?
13) Какие меры защиты применяются для предотвращения утечки информации через периферийные устройства?
14) Как оценить эффективность системы информационной защиты в производственном подразделении?
15) Какие риски возникают при использовании облачных технологий в производственных подразделениях?
16) Как организовать резервное копирование данных в производственных подразделениях и обеспечить их защиту?
17) Какие методы аутентификации и авторизации используются в системах защиты информации на производстве?
18) Как обеспечить защиту информации от вредоносного программного обеспечения в автоматизированных системах?
19) Какие особенности защиты информации в промышленных системах управления (ICS/SCADA)?
20) Как организовать обучение сотрудников производственных подразделений по вопросам информационной безопасности?

2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы (оцениваемые знания, умения,

компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие основные задачи решаются в процессе технической эксплуатации элементов программной и аппаратной защиты автоматизированных систем?
2) Какие виды аппаратных средств защиты информации используются в автоматизированных системах?
3) Как осуществляется мониторинг работоспособности программных средств защиты информации?
4) Какие этапы включает процесс технического обслуживания аппаратных средств защиты?
5) Как провести диагностику неисправностей в работе программно-аппаратных средств защиты?
6) Какие меры безопасности необходимо соблюдать при эксплуатации аппаратных средств защиты информации?
7) Как организовать обновление программного обеспечения средств защиты информации?
8) Какие методы используются для тестирования работоспособности элементов защиты автоматизированной системы?
9) Как обеспечить резервирование и восстановление данных при эксплуатации систем защиты?
10) Какие документы необходимы для ведения учета технической эксплуатации средств защиты информации?
11) Как осуществляется настройка параметров работы программно-аппаратных средств защиты?
12) Какие действия необходимо выполнить при обнаружении уязвимостей в элементах защиты автоматизированной системы?
13) Как организовать контроль доступа к аппаратным средствам защиты информации?
14) Какие инструменты используются для диагностики и устранения сбоев в работе программных средств защиты?
15) Как обеспечить совместимость программных и аппаратных средств защиты с другими компонентами автоматизированной системы?
16) Какие меры принимаются для защиты аппаратных средств от физического повреждения или несанкционированного доступа?
17) Как организовать регулярное техническое обслуживание программно-аппаратных средств защиты?
18) Какие методы применяются для защиты данных при передаче между элементами автоматизированной системы?

19) Как обеспечить безопасность данных при эксплуатации резервных копий в автоматизированных системах?
20) Какие действия необходимо выполнить при выводе из эксплуатации устаревших элементов программной или аппаратной защиты?

3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие основные этапы включает процесс диагностирования отказов программно-аппаратных средств обеспечения информационной безопасности?
2) Какие инструменты и методы используются для диагностики неисправностей в работе программно-аппаратных средств защиты?
3) Как определить причину отказа в работе аппаратного средства обеспечения информационной безопасности?
4) Какие действия необходимо выполнить при обнаружении сбоя в работе программного средства защиты информации?
5) Как организовать процесс восстановления работоспособности программно-аппаратных средств после отказа?
6) Какие меры безопасности необходимо соблюдать при устранении отказов в работе средств защиты информации?
7) Как провести тестирование работоспособности программно-аппаратных средств после устранения отказа?
8) Какие документы необходимо заполнять при диагностировании и устранении отказов средств защиты информации?
9) Как обеспечить минимизацию времени простоя автоматизированной системы при устранении отказов?
10) Какие методы применяются для предотвращения повторных отказов программно-аппаратных средств защиты?
11) Как организовать мониторинг работоспособности программно-аппаратных средств обеспечения информационной безопасности?
12) Какие действия необходимо выполнить при обнаружении уязвимости в работе средств защиты информации?
13) Как обеспечить резервирование данных и настроек при устранении отказов в работе средств защиты?
14) Какие меры принимаются для защиты данных при диагностировании и

устранении отказов в автоматизированных системах?

15) Как организовать взаимодействие с производителями оборудования или программного обеспечения при устранении сложных отказов?
16) Какие методы применяются для восстановления данных после сбоя в работе средств защиты информации?
17) Как обеспечить совместимость обновленных или восстановленных средств защиты с другими компонентами автоматизированной системы?
18) Какие действия необходимо выполнить при выводе из эксплуатации неисправных программно-аппаратных средств защиты?
19) Как организовать обучение сотрудников по вопросам диагностирования и устранения отказов средств защиты информации?
20) Какие меры принимаются для предотвращения несанкционированного доступа к данным в процессе устранения отказов?

4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие критерии используются для оценки эффективности программно-аппаратных средств обеспечения информационной безопасности?
2) Как определить, соответствуют ли применяемые средства защиты информации требованиям нормативных документов?
3) Какие методы применяются для анализа уровня защищенности данных в структурном подразделении?
4) Как оценить степень устойчивости программно-аппаратных средств к кибератакам?
5) Какие показатели эффективности используются при анализе работы средств защиты информации?
6) Как провести аудит используемых программно-аппаратных средств обеспечения информационной безопасности?
7) Какие инструменты и программные средства применяются для анализа эффективности защиты информации?
8) Как определить, насколько эффективно средства защиты предотвращают утечку данных?
9) Какие действия необходимо выполнить при выявлении недостатков в работе программно-аппаратных средств защиты?
10) Как оценить уровень совместимости применяемых средств защиты с

другими системами в структурном подразделении?

11) Какие методы используются для анализа затрат на эксплуатацию средств защиты информации?
12) Как определить, насколько эффективно средства защиты справляются с новыми угрозами информационной безопасности?
13) Какие меры принимаются для повышения эффективности работы программно-аппаратных средств защиты?
14) Как организовать сбор и анализ данных о сбоях и отказах в работе средств защиты информации?
15) Какие действия необходимо выполнить для оптимизации работы программно-аппаратных средств защиты?
16) Как оценить уровень удовлетворенности пользователей работой средств защиты информации?
17) Какие методы применяются для анализа уровня подготовки сотрудников к работе с программно-аппаратными средствами защиты?
18) Как определить, насколько эффективно средства защиты обеспечивают конфиденциальность, целостность и доступность данных?
19) Какие действия необходимо выполнить для подготовки отчета об эффективности применяемых средств защиты информации?
20) Как организовать внедрение улучшений на основе анализа эффективности программно-аппаратных средств защиты?

5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие основные принципы лежат в основе учета конфиденциальной информации в автоматизированных системах?
2) Какие методы и средства используются для защиты конфиденциальной информации при ее обработке?
3) Как организовать безопасное хранение конфиденциальной информации в автоматизированных системах?
4) Какие меры защиты применяются при передаче конфиденциальной информации между подразделениями или внешними организациями?
5) Какие нормативные документы регулируют учет и обработку конфиденциальной информации?
6) Как обеспечить контроль доступа к конфиденциальной информации на этапах ее учета и обработки?

7) Какие методы шифрования применяются для защиты конфиденциальной информации при передаче?
8) Как организовать резервное копирование конфиденциальной информации и обеспечить ее защиту?
9) Какие действия необходимо выполнить при обнаружении утечки конфиденциальной информации?
10) Как обеспечить целостность конфиденциальной информации при ее хранении и передаче?
11) Какие программно-аппаратные средства используются для защиты конфиденциальной информации в автоматизированных системах?
12) Как организовать учет доступа сотрудников к конфиденциальной информации?
13) Какие меры принимаются для защиты конфиденциальной информации от несанкционированного копирования или удаления?
14) Как обеспечить безопасность конфиденциальной информации при использовании облачных технологий?
15) Какие методы применяются для аутентификации и авторизации при доступе к конфиденциальной информации?
16) Как организовать мониторинг процессов обработки и передачи конфиденциальной информации?
17) Какие действия необходимо выполнить при выводе из эксплуатации носителей конфиденциальной информации?
18) Как обеспечить защиту конфиденциальной информации от вредоносного программного обеспечения?
19) Какие меры принимаются для предотвращения утечки конфиденциальной информации через периферийные устройства?
20) Как организовать обучение сотрудников по вопросам работы с конфиденциальной информацией?

6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики (оцениваемые знания, умения, компетенции: З1-9, У1-6, ПО1-8, ОК1-10, ПК 2.1-2.6)

Вопросы:

1) Какие нормативные правовые акты регулируют обеспечение информационной безопасности в Российской Федерации?
2) Какой документ определяет требования к защите информации в автоматизированных системах?

3) Какие положения Федерального закона № 152-ФЗ "О персональных данных" необходимо учитывать при обеспечении информационной безопасности?
4) Какие нормативные документы регламентируют использование программно-аппаратных средств защиты информации?
5) Как применяются стандарты ГОСТ Р в области информационной безопасности при выполнении задач практики?
6) Какие требования к защите информации содержатся в нормативных методических документах ФСТЭК России?
7) Как обеспечить соответствие автоматизированной системы требованиям нормативных документов по информационной безопасности?
8) Какие действия необходимо выполнить для сертификации программно-аппаратных средств защиты информации?
9) Как применяются международные стандарты информационной безопасности (например, ISO/IEC 27001) в российской практике?
10) Какие нормативные документы регулируют защиту информации в критически важных объектах инфраструктуры?
11) Как организовать работу с конфиденциальной информацией в соответствии с нормативными правовыми актами?
12) Какие меры защиты информации предписываются нормативными документами для автоматизированных систем обработки персональных данных?
13) Как обеспечить выполнение требований нормативных документов при выборе программно-аппаратных средств защиты информации?
14) Какие нормативные документы регулируют защиту информации в государственных информационных системах?
15) Как применяются методические рекомендации ФСБ России при обеспечении информационной безопасности?
16) Какие действия необходимо выполнить для проведения аудита информационной безопасности в соответствии с нормативными требованиями?
17) Как обеспечить защиту информации от несанкционированного доступа в соответствии с нормативными документами?
18) Какие нормативные документы регулируют использование криптографических средств защиты информации?
19) Как организовать обучение сотрудников по вопросам соблюдения нормативных требований в области информационной безопасности?
20) Какие меры ответственности предусмотрены за нарушение нормативных правовых актов в области информационной безопасности?

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 (неудовлетворительно)	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

перечень учебных изданий, электронных изданий, электронных и Интернет- ресурсов, образовательных платформ, электронно-библиотечных систем, веб- систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Ильин М. Е., Калинкина Т. И., Пржегорлинский В.Н. Криптографическая защита информации в объектах информационной инфраструктуры, 1-е изд., 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 г

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 недекларированных 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 с

использованием средств криптографической защиты информации ограниченным доступом, не содержащей 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 Автоматизированные системы в защищенном исполнении. Защита информации. 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 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

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.

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

48. 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 криптологии: 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. 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. 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

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 PROFобразование:

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