



IThub
college



Caspian

Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд. 18м
ОГРН: 1220500003580, ИНН: 0572030404

КОМПЛЕКТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНЫХ И ПРОИЗВОДСТВЕННЫХ ПРАКТИК

по специальности

**10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**
квалификация
техник по защите информации

Махачкала, 2025

1. Основные требования к отчетной документации по практике

по учебной практике:

- ✓ краткий отчет/отчеты по практическим работам/портфолио (при прохождении практики в Колледже КАСПИЙ) на платформе LXP;
- ✓ дневник (при прохождении практики в Профильной организации);

по производственной практике по виду деятельности и производственной практике (преддипломной):

- ✓ дневник;
- ✓ характеристику на обучающегося с места практики;
- ✓ отчет по практике;
- ✓ портфолио – приложение к отчету *по производственной практике (по виду деятельности)*, содержащее документы и материалы, подтверждающие выполненные работы и профессиональную деятельность обучающегося в период практики (текстовый, графический, фото-, видео-, аудиоматериал, макет и др.).

Все указанные документы могут быть представлены в электронном виде, с утверждением электронной подписью руководителя Профильной организации.

Содержательная часть отчета по практике отражает следующие вопросы:

- общие сведения о Профильной организации (наименование, правовой статус, наличие филиалов и представительств, краткая история развития, краткая характеристика основных видов деятельности); описание организационной структуры управления организацией (можно отобразить схематично);
- описание функций подразделения, в котором студент проходил практику, и структуру управления подразделением с распределением обязанностей, в том числе – по должности, которую занимал во время практики обучающийся (для преддипломной практики);
- описание изученных в ходе практики материалов;
- подробное описание выполненных работ на основании дневника практики.

Характеристика с места практики должна содержать предлагаемую оценку за практическую деятельность обучающегося, заверенную подписью руководителя практики от профильной организации и печатью.

На основании представленных отчетных документов руководитель практики от Колледжа КАСПИЙ заполняет на каждого обучающегося Аттестационный лист с последующей передачей его в Учебную часть.

Аттестационный лист содержит сведения об уровне освоения обучающимся профессиональных компетенций,

Руководитель кафедрой формирует сводный отчет о прохождении практики обучающимися и сдает его заместителю директора по индустриальному направлению вместе с отчетами по практике обучающихся.

2. Особенности проведения практики

2.1. Особенности проведения практики с использованием дистанционных образовательных технологий

Программы учебной и/или производственной практик или отдельные части программ могут быть реализованы в дистанционном режиме (с использованием дистанционных образовательных технологий – ДОТ).

Решение о возможности прохождения практики в удаленном формате принимается Колледжем КАСПИЙ по согласованию с Профильной организацией – базой практики.

Обучающиеся могут проходить учебную и/или производственную практику удаленно, выполняя практические задания под руководством руководителя практики от образовательной организации и производственные задания – под руководством руководителя практики от Профильной организации (предприятия).

Приказ о направлении обучающихся на прохождение практики удаленно доводится до сведения руководителей преддипломной практики с помощью электронных ресурсов.

При организации прохождения учебной практики с использованием ДОТ на образовательной платформе «LXP IThub» в разделе «Учебная практика» размещаются кейсы (задачи) от внутренних подразделений образовательной организации, решение которых направлено на приобретение практического опыта на основании изучения комплекса дисциплин и междисциплинарных курсов практик, соответствующего определенному виду деятельности будущего специалиста. Решение кейса должно быть оформлено и выложено обучающимся на платформе.

При организации прохождения производственной практики с использованием ДОТ на образовательной платформе «LXP IThub» в разделе «Производственная практика» размещаются кейсы (задачи) смоделированных условий, ситуаций, максимально приближенных к реальным производственным условиям, от компаний-партнеров, решение которых должно быть оформлено и выложено на платформе в виде ссылки в личном кабинете веб-сервиса (например, GitHub или Behance).

Взаимодействие руководителя практики и обучающихся происходит исключительно с применением ДОТ.

Отчетные материалы по практике предоставляются обучающимся руководителю практики от Колледжа КАСПИЙ в электронном виде через образовательную платформу или по электронной почте на следующий день после окончания практики, без последующего предоставления в бумажном варианте. Допускается не проставление оттиска печати и подписи руководителя практики от Профильной организации на отчетную документацию по производственной практике в случае прохождения ее в дистанционном формате.

Отчетность по производственной практике обучающихся хранится в учебной части на электронных носителях.

Отчетная (зачетная) ведомость учебной и/или производственной практике оформляется руководителем от образовательной организации в электронном виде и на бумажном носителе.

Аттестационный лист обязательно заполняется на бумажном носителе, т.к. участвует в отчете по модулю.

3. Порядок проведения практики для инвалидов и лиц с ограниченными возможностями

здоровья (ОВЗ)

Для студентов - инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) форма проведения практики устанавливается с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

Выбор мест прохождения практик для инвалидов и лиц с ОВЗ производится с учетом требований их доступности для данных обучающихся и рекомендации медико-социальной экспертизы, а также индивидуальной программы реабилитации инвалида, относительно рекомендованных условий и видов труда.

Индивидуальная программа реабилитации инвалида выдается федеральным государственным учреждением медико-социальной экспертизы. Инвалид или лицо с ОВЗ предоставляют рекомендации медико-социальной экспертизы, индивидуальную программу реабилитации по своему усмотрению при приеме на обучение.

При направлении инвалида и обучающегося с ОВЗ в Профильную организацию или предприятие для прохождения предусмотренной учебным планом практики образовательная организация согласовывает с Профильной организацией (предприятием) условия и виды труда с учетом рекомендаций медико-социальной экспертизы и индивидуальной программы реабилитации инвалида. При необходимости для прохождения практик студентами-инвалидами или лицами с ОВЗ могут создаваться специальные рабочие места в соответствии с характером нарушений, а также с учетом вида деятельности и характера труда, выполняемых обучающимся инвалидом трудовых функций.

**Контрольно-оценочные средства УП и ПП.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
разработаны в соответствии с
ФГОС 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Комплект контрольно-оценочных средств (КОС) практик разработан на основе:

- Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- программы учебной и производственной практик УП и ПП.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Комплект контрольно-оценочных средств предназначен для оценки результатов освоения УП и ПП.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Результатом освоения практик является готовность обучающегося к выполнению вида профессиональной деятельности «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» и формирование практического опыта, умений, знаний, профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ОПОП в целом.

В результате освоения дисциплины студент овладеет:

Код ОК и ПК	Умения	Знания
ОК 01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации

	составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы.	и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации.
ОК 04	организовывать работу коллектива и команды взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива психологические особенности личности
ПК 1.1	осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем.	состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств.
ПК 1.2	организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы.	теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации.
ПК 1.3	настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.	порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.
ПК 1.4	обеспечивать работоспособность, обнаруживать и устранять неисправности.	принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.
ПК 1.5д	умение идентифицировать и анализировать возможные угрозы и	основные понятия, термины и принципы управления рисками в

	уязвимости информационных систем; умение проводить качественную и количественную оценку рисков информационной безопасности; умение выявлять и интерпретировать кризисные индикаторы, сигнализирующие о нарушении информационной безопасности.	области информационной безопасности; методологии и стандарты оценки рисков; классификация угроз, уязвимостей и источников угроз в сфере информационной безопасности.
ПК 1.6д	выявлять и классифицировать инциденты информационной безопасности: проводить первичный и углубленный анализ инцидентов с использованием логов, систем мониторинга и анализа; организовывать и выполнять техническое расследование инцидентов ИБ.	этапы жизненного цикла инцидента ИБ: обнаружение, анализ, локализация, устранение, восстановление, анализ после инцидента; составляющие системы управления инцидентами ИБ: политики, процедуры, роли, каналы коммуникации, планы реагирования.
ПК 1.7д	выполнять установку, конфигурирование и верификацию настроек средств защиты информации в составе информационных систем в соответствии с технической документацией и регламентами безопасности	принципы, методы и нормативные требования по обеспечению информационной безопасности при развёртывании и эксплуатации информационных систем, включая порядок применения средств защиты информации.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной и производственной практик должен:

Иметь опыт:

- установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
- администрирование автоматизированных систем в защищенном исполнении
- эксплуатация компонентов систем защиты информации автоматизированных систем
- диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
- работы с матрицами оценки вероятности и воздействия рисков (матрица рисков); подготовки отчетов по результатам оценки рисков и кризисным индикаторам; применения моделей и сценариев развития угроз при анализе рисков
- подготовки рекомендаций по предотвращению повторного возникновения аналогичных инцидентов; моделирования сценариев возможных атак и проверки готовности системы реагирования
- развёртывания и сопровождения информационных систем в защищённом исполнении с применением сертифицированных средств защиты и контролем соблюдения политик безопасности

Типовые вопросы для оценки результатов учебной и производственной практики

Раздел 1. Вопросы по профессиональным компетенциям (ПК)

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении

в соответствии с требованиями эксплуатационной документации

1. Опишите процесс установки и первоначальной настройки защищённой ОС (например, Astra Linux или Windows Server с политиками ИБ) в рамках вашей практики.
2. Какие требования эксплуатационной документации вы учитывали при настройке СУБД с функциями защиты?
3. Продемонстрируйте конфигурационные файлы или скрипты, использованные вами для развёртывания защищённого компонента ИС, и обоснуйте выбор параметров безопасности.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении

4. Опишите задачи администрирования, выполненные вами в ходе практики (управление пользователями, политиками, обновлениями, резервным копированием).
5. Как вы обеспечивали безопасность при администрировании сетевых сервисов (SSH, RDP, веб-интерфейсы)?
6. Продемонстрируйте пример настройки аппаратного модуля безопасности (HSM, TPM) или программно-аппаратного комплекса.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

7. Какие меры вы применяли для обеспечения отказоустойчивости и непрерывности работы ИС?
8. Опишите организацию мониторинга доступности и производительности защищённой ИС.
9. Как вы проверяли соответствие эксплуатации системы требованиям регламентирующих документов (ГОСТ, ФСТЭК)?

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

10. Приведите пример диагностики и устранения сбоя в работе защищённой системы (например, отказ СУБД, сетевой инцидент).
11. Какие инструменты вы использовали для проверки технического состояния оборудования и ПО?
12. Опишите процедуру восстановления системы после сбоя с учётом требований информационной безопасности.

ПК 1.5д. Осуществлять оценку рисков и кризисных индикаторов информационной безопасности

13. Проведите анализ угроз для защищаемой ИС, с которой вы работали, и опишите выявленные риски.
14. Какие кризисные индикаторы ИБ вы отслеживали в ходе практики?
15. Продемонстрируйте шаблон или отчёт по оценке рисков, подготовленный вами.

ПК 1.6д. Выполнять работы по расследованию инцидентов информационной безопасности и выстраивание процессов реагирования на инциденты

16. Опишите смоделированный или реальный инцидент ИБ, с которым вы работали, и ваши действия по его расследованию.
17. Какие данные (логи, дампы, артефакты) вы анализировали при расследовании?

18. Продемонстрируйте разработанный вами план реагирования на инцидент ИБ (IRP).

ПК 1.7д. Осуществлять установку, настройку и поддержку эксплуатации информационных систем в защищённом исполнении

19. Опишите выполненную вами установку и настройку средств защиты информации в составе информационной системы в защищённом исполнении.
20. Как вы проводили верификацию настроек средств защиты информации на соответствие технической документации и регламентам безопасности?
21. Продемонстрируйте регламент или чек-лист сопровождения эксплуатации защищённой информационной системы, подготовленный или применённый вами.

Раздел 2. Вопросы по общим компетенциям (ОК)

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

19. Опишите ситуацию, в которой вам пришлось выбрать между несколькими техническими решениями по защите ИС. Обоснуйте ваш выбор.
20. Как вы учитывали контекст (тип организации, уровень секретности, ресурсы) при принятии решений?

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

21. Какие ИТ-инструменты и платформы вы использовали в ходе практики (SIEM, WAF, IDS, административные панели)?
22. Приведите пример использования профессиональных источников (CVE, MITRE ATT&CK, документация ФСТЭК) для решения задачи.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

23. Опишите вашу роль в командной работе при выполнении практики и пример успешного взаимодействия.
24. Как вы распределяли задачи и координировали действия с другими участниками практики?

Раздел 3. Комплексные практические задания

Для учебной практики:

29. Установите и настройте защищённую виртуальную ИС (включая ОС, СУБД, веб-сервер) в соответствии с требованиями ФСТЭК.
30. Настройте систему мониторинга и логирования (например, ELK-стек или аналог) для сбора и анализа событий безопасности.
31. Проведите базовую оценку рисков для развернутой ИС и предложите меры по снижению выявленных угроз.

Для производственной практики:

32. Администрируйте защищённую ИС в реальной или максимально приближенной к реальной среде в течение недели, обеспечивая её стабильную работу.
33. Проанализируйте журналы событий за сутки, выявите подозрительную активность и оформите отчёт по инциденту ИБ.
34. Разработайте и внедрите улучшения в процессы эксплуатации ИС (например, автоматизация резервного копирования, обновление политик доступа, настройка аудита).

Критерии оценки:

Критерий	5	4	3	2
Установка и настройка компонентов СЗИ (ПК 1.1)	Устанавливает и настраивает компоненты систем защиты информации АС в полном соответствии с требованиями ИБ и эксплуатационной документации; все параметры заданы и проверены.	Устанавливает и настраивает компоненты СЗИ в основном корректно; допущены отдельные упрощения, не критичные для ИБ.	Выполняет базовую установку компонентов СЗИ без части ключевых мер защиты; имеются нарушения требований ИБ.	Не устанавливает и не настраивает компоненты СЗИ либо допускает грубые нарушения требований ИБ.
Администрирование АС в защищённом исполнении (ПК 1.2)	Администрирует АС в защищённом исполнении в полном объёме (пользователи, политики, обновления, резервное копирование); ведёт комплексный контроль.	Администрирует АС в защищённом исполнении; отдельные операции выполнены вручную, меры ИБ применены не в полном объёме.	Выполняет только базовые операции администрирования; автоматизация и защита реализованы слабо.	Администрирование не выполнено либо привело к сбою или утечке.
Эксплуатация компонентов СЗИ (ПК 1.3)	Обеспечивает бесперебойную эксплуатацию компонентов СЗИ АС; настроены мониторинг, резервирование и отказоустойчивость, работоспособность подтверждена при тестировании.	Эксплуатирует компоненты СЗИ; непрерывность обеспечена, но без полного резервирования или автоматического восстановления.	Поддерживает работу компонентов СЗИ только в штатном режиме; при сбое возможен простой.	Бесперебойная эксплуатация не обеспечена; меры поддержания непрерывности отсутствуют.
Диагностика и восстановление работоспособности (ПК 1.4)	Проводит диагностику компонентов СЗИ, устраняет отказы и восстанавливает работоспособность АС в защищённом исполнении; причина отказа выявлена и устранена.	Устраняет отказ, но без глубокого анализа причин; восстановление выполнено.	Выполняет перезапуск и восстановление без диагностики; надёжность восстановления невысокая.	Отказ не устранён либо действия усугубили ситуацию.
Оценка рисков и кризисных индикаторов ИБ (ПК 1.5д)	Проводит оценку рисков ИБ с использованием матрицы рисков, готовит отчёты по результатам оценки и кризисным индикаторам, применяет модели и сценарии развития угроз.	Проводит оценку рисков, но без приоритизации; меры и отчётность общие.	Перечисляет угрозы шаблонно, без привязки к системе и без сценариев.	Оценка рисков не проведена либо выполнена ошибочно.
Расследование инцидентов и реагирование (ПК 1.6д)	Выполняет анализ инцидента, готовит рекомендации по предотвращению повторных инцидентов, моделирует сценарии атак и проверяет готовность системы реагирования.	Инцидент проанализирован, отчёт составлен, но без детального плана реагирования (IRP).	Фиксирует инцидент без анализа; рекомендации и моделирование отсутствуют.	Расследование и реагирование не проведены.
Развёртывание и сопровождение защищённых ИС (ПК 1.7д)	Развёртывает и сопровождает информационные системы в защищённом исполнении с применением сертифицированных СЗИ; контролирует	Развёртывает и сопровождает ИС; контроль соблюдения политик безопасности выполнен не в полном объёме.	Выполняет развёртывание частично; сертифицированные СЗИ и контроль политик применены ограниченно.	Развёртывание и сопровождение не выполнены либо политики безопасности нарушены.

	соблюдение политик безопасности.			
Выбор способов решения профессиональных задач (ОК 01)	Обоснованно выбирает способы решения задач профессиональной деятельности применительно к различным контекстам.	Выбирает способ решения задачи, но обоснование неполное.	Выбирает решение шаблонно, без учёта контекста.	Не способен выбрать адекватный способ решения задачи.
Поиск, анализ и интерпретация информации (ОК 02)	Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для решения профессиональных задач.	Использует средства поиска и анализа информации, но анализ упрощён.	Применяет базовые средства поиска; анализ поверхностный.	Современные средства поиска и анализа информации не применяет.

**Контрольно-оценочные средства по УП и ПП.02 Защита информации в
автоматизированных системах программными и программно-аппаратными
средствами
разработаны в соответствии с
ФГОС 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Комплект контрольно-оценочных средств (КОС) практик разработан на основе:

- Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- программы учебной и производственной практик УП и ПП.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Комплект контрольно-оценочных средств предназначен для оценки результатов освоения УП и ПП.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Результатом освоения практик является готовность обучающегося к выполнению вида профессиональной деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и формирование практического опыта, умений, знаний, профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ОПОП в целом.

В результате освоения дисциплины студент овладеет:

Код ОК и ПК	Умения	Знания
ОК 01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы.	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации.
ОК 04	организовывать работу коллектива и команды взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива психологические особенности личности

ПК 2.1	анализировать проектную и техническую документацию; использовать специализированные графические средства построения и анализа архитектуры программных продуктов; организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов; определять источники и приемники данных; проводить сравнительный анализ; выполнять отладку, используя методы и инструменты условной компиляции (классы Debug и Trace); оценивать размер минимального набора тестов; разрабатывать тестовые пакеты и тестовые сценарии; выявлять ошибки в системных компонентах на основе спецификаций.	модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; виды и варианты интеграционных решений; современные технологии и инструменты интеграции; основные протоколы доступа к данным; методы и способы идентификации сбоев и ошибок при интеграции приложений; методы отладочных классов; стандарты качества программной документации; основы организации инспектирования и верификации; встроенные и основные специализированные инструменты анализа качества программных продуктов; графические средства проектирования архитектуры программных продуктов; методы организации работы в команде разработчиков.
ПК 2.2	использовать выбранную систему контроля версий; использовать методы для получения кода с заданной функциональностью и степенью качества; организовывать заданную интеграцию модулей в программные средства на базе имеющейся архитектуры и автоматизации бизнес-процессов; использовать различные транспортные протоколы и стандарты форматирования сообщений; выполнять тестирование интеграции; организовывать постобработку данных; создавать классы-исключения на основе базовых классов; выполнять ручное и автоматизированное тестирование программного модуля; выявлять ошибки в системных компонентах на основе спецификаций; использовать приемы работы в системах контроля версий.	модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; основы верификации программного обеспечения; современные технологии и инструменты интеграции; основные протоколы доступа к данным; методы и способы идентификации сбоев и ошибок при интеграции приложений; основные методы отладки; методы и схемы обработки исключительных ситуаций; основные методы и виды тестирования программных продуктов; стандарты качества программной документации; основы организации инспектирования и верификации; приемы работы с инструментальными средствами тестирования и отладки; методы организации работы в команде разработчиков.
ПК 2.3	использовать выбранную систему контроля версий; использовать методы для получения кода с заданной функциональностью и степенью качества; анализировать проектную и техническую документацию; использовать инструментальные средства отладки программных продуктов; определять источники и приемники данных; выполнять тестирование интеграции; организовывать постобработку данных; использовать приемы работы в системах контроля версий; выполнять отладку, используя методы и инструменты условной компиляции; выявлять ошибки в системных компонентах на основе спецификаций.	модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; основы верификации и аттестации программного обеспечения; методы и способы идентификации сбоев и ошибок при интеграции приложений; основные методы отладки; методы и схемы обработки исключительных ситуаций; приемы работы с инструментальными средствами тестирования и отладки; стандарты качества программной документации; основы организации инспектирования и верификации; встроенные и основные специализированные инструменты анализа качества программных продуктов; методы организации работы в команде

		разработчиков.
ПК 2.4	использовать выбранную систему контроля версий; анализировать проектную и техническую документацию; выполнять тестирование интеграции; организовывать постобработку данных; использовать приемы работы в системах контроля версий; оценивать размер минимального набора тестов; разрабатывать тестовые пакеты и тестовые сценарии; выполнять ручное и автоматизированное тестирование программного модуля; выявлять ошибки в системных компонентах на основе спецификаций.	модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; основы верификации и аттестации программного обеспечения; методы и способы идентификации сбоев и ошибок при интеграции приложений; методы и схемы обработки исключительных ситуаций; основные методы и виды тестирования программных продуктов; приемы работы с инструментальными средствами тестирования и отладки; стандарты качества программной документации; основы организации инспектирования и верификации; встроенные и основные специализированные инструменты анализа качества программных продуктов; методы организации работы в команде разработчиков.
ПК 2.5	применять средства гарантированного уничтожения информации.	особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации.
ПК 2.6	устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; 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.	типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.
ПК 2.7д	анализировать уязвимости информационных систем и прогнозировать возможные атаки злоумышленников; разрабатывать архитектуру комплексной системы защиты информации на основе анализа рисков.	современных видов и методов кибератак, используемых злоумышленниками; знание архитектур и принципов построения систем защиты информации (СЗИ); знание классификации средств защиты информации: программные, аппаратные, программно-аппаратные.
ПК 2.8д	выявлять признаки и предпосылки инцидентов, связанных с социальной инженерией; анализировать ситуации, в которых возможно использование методов социальной инженерии, и оценивать связанные риски.	понятия и виды социальной инженерии; психологические принципы и тактики манипуляции, используемые злоумышленниками в целях получения конфиденциальной информации; стандарты и подходы к обеспечению информационной безопасности при взаимодействии с персоналом.
ПК 2.9д	применять программно-аппаратные средства защиты информации для организации регламентированного доступа, контроля целостности и предотвращения утечек сведений ограниченного доступа	нормативно-правовые акты, регламенты и методики по защите информации ограниченного доступа, а также принципы функционирования программно-аппаратных средств обеспечения информационной безопасности

С целью овладения указанным видом профессиональной деятельности и

соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной и производственной практик должен:

Иметь опыт:

- установка, настройка программных средств защиты информации в автоматизированной системе
- обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети
- тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации
- решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
- учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
- работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе
- использования методологий безопасной разработки ПО и проектирования защищённых архитектур; работы с инструментами тестирования на проникновение (pentest), анализа уязвимостей и сканирования безопасности
- применения технических и организационных мер защиты от социальной инженерии; моделирования атак с применением методов социальной инженерии для проверки уровня защищённости организации
- организации рабочих мест и процессов обработки информации ограниченного доступа с использованием сертифицированных средств защиты и соблюдением требований режимных мероприятий

Типовые вопросы для оценки результатов учебной и производственной практики

Раздел 1. Вопросы по профессиональным компетенциям (ПК)

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

1. Опишите процесс установки и первоначальной настройки программного средства защиты (например, межсетевого экрана, DLP-системы или HSM).
2. Какие требования сертификации и эксплуатационной документации вы учитывали при настройке?
3. Продемонстрируйте конфигурационные файлы или скриншоты интерфейса и обоснуйте выбор параметров безопасности.

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

4. Какие средства защиты вы применяли для обеспечения конфиденциальности, целостности и доступности данных в ИС?
5. Продемонстрируйте пример интеграции программно-аппаратного средства (например, криптографического модуля) в защищаемую систему.
6. Как вы проверяли корректность работы средств защиты после их внедрения?

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

7. Опишите разработанный вами тестовый сценарий для проверки функций средства защиты (например, фильтрации трафика, шифрования, аудита).

8. Какие инструменты вы использовали для генерации тестового трафика или эмуляции атак?
9. Продемонстрируйте отчёт по результатам тестирования с выводами и рекомендациями.

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

10. Какие меры вы применяли при работе с персональными данными или иной информацией ограниченного доступа?
11. Опишите организацию защищённого хранения (шифрование, доступ, резервное копирование) и передачи (VPN, TLS, защищённые протоколы).
12. Как вы обеспечивали соответствие требованиям Ф3-152 и других нормативных актов?

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

13. Какие методы уничтожения данных вы применяли (программное затирание, криптографическое обнуление, физическое уничтожение)?
14. Продемонстрируйте протокол уничтожения информации, включая подтверждающие артефакты (логи, акты).
15. Как вы проверяли эффективность уничтожения данных?

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

16. Какие системы мониторинга и регистрации событий вы настраивали (SIEM, IDS/IPS, аудит ОС)?
17. Продемонстрируйте пример корреляционного правила или сигнатуры, созданной вами для обнаружения атаки.
18. Как вы организовывали архивирование и защиту журналов событий?

ПК 2.7д. Противостоять действиям злоумышленников при помощи проектирования средств и методов защиты информационных систем

19. Опишите архитектурное решение по защите ИС, разработанное вами для противодействия конкретной угрозе (например, APT, DDoS, insider threat).
20. Какие методы защиты (сегментация, Zero Trust, микросегментация) вы применяли и почему?
21. Продемонстрируйте схему защиты с комментариями по уровням и компонентам.

ПК 2.8д. Противодействовать инцидентам информационной безопасности, основанным на методах социальной инженерии

22. Какие технические и организационные меры вы предложили для защиты от фишинга, вишинга, имперсонации?
23. Опишите смоделированный сценарий социальной инженерии и ваши действия по его предотвращению/реагированию.
24. Как вы проводили обучение пользователей или проверяли их устойчивость к подобным атакам?

ПК 2.9д. Организовывать безопасную работу с информацией ограниченного доступа, в т.ч. программно-аппаратными средствами

25. Опишите, как вы организовывали регламентированный доступ к информации ограниченного доступа в ходе практики.
26. Какие программно-аппаратные средства вы применяли для контроля целостности и предотвращения утечек сведений ограниченного доступа?

27. Продемонстрируйте настройку разграничения доступа или средства предотвращения утечек и обоснуйте её соответствие нормативным требованиям.

Раздел 2. Вопросы по общим компетенциям (ОК)

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

25. Опишите ситуацию, в которой вам пришлось выбирать между несколькими средствами защиты (например, DLP vs. шифрование). Обоснуйте ваш выбор.
26. Как вы учитывали специфику организации (бюджет, уровень секретности, инфраструктуру) при принятии решений?

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

27. Какие профессиональные инструменты вы использовали (Wireshark, Nmap, Metasploit, OSSEC, Hashcat и др.) и для каких задач?
28. Приведите пример анализа угроз с использованием открытых источников (CVE, MITRE ATT&CK, VirusTotal).

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

29. Опишите вашу роль в командной работе при выполнении практики (например, совместная настройка SOC или пентест).
30. Как вы распределяли задачи и координировали действия с коллегами или наставником?

Раздел 3. Комплексные практические задания

Для учебной практики:

35. Установите, настройте и протестируйте программное средство защиты (например, WAF, антивирус, DLP) в лабораторной среде.
36. Настройте систему регистрации событий (например, на базе ELK или аналога) и создайте правила обнаружения атак.
37. Проведите моделирование инцидента социальной инженерии и разработайте план противодействия.

Для производственной практики:

38. Внедрите программно-аппаратное средство защиты (например, HSM или защищённый аутентификатор) в реальную или максимально приближённую к реальной ИС.
39. Проведите комплексное тестирование средств защиты ИС: функциональность, отказоустойчивость, устойчивость к атакам.
40. Разработайте и реализуйте меры по защите информации ограниченного доступа в соответствии с требованиями заказчика или регулятора.

Критерии оценки:

Критерий	5	4	3	2
Установка и настройка программных СЗИ (ПК 2.1)	Устанавливает и настраивает программные средства защиты информации в АС в полном соответствии с требованиями; все средства настроены и проверены.	Устанавливает и настраивает программные СЗИ с отдельными недочётами.	Выполняет базовую настройку программных СЗИ без учёта части требований.	Программные СЗИ не установлены или настроены неверно.
Защита автономных АС и сетей (ПК 2.2)	Обеспечивает защиту автономных АС и защиту информации в сети программными и программно-аппаратными средствами в комплексе.	Обеспечивает защиту, но задействованы не все механизмы.	Применяет отдельные меры защиты без системного подхода.	Защита не обеспечена; нарушены базовые требования ИБ.
Тестирование и восстановление СЗИ (ПК 2.3)	Тестирует функции, проводит диагностику, устраняет отказы и восстанавливает работоспособность программных и программно-аппаратных СЗИ.	Тестирует и восстанавливает СЗИ, но без глубокой диагностики.	Выполняет только базовую проверку функций СЗИ.	Тестирование и восстановление не выполнены.
Защита от НСД и криптозащита (ПК 2.4)	Решает задачи защиты от НСД к информации ограниченного доступа, применяет электронную подпись, симметричные и асимметричные криптоалгоритмы и средства шифрования.	Решает задачи защиты от НСД, но применение криптосредств неполное.	Применяет отдельные средства защиты от НСД без шифрования.	Защита от НСД и криптозащита не реализованы.
Работа с конфиденциальной информацией (ПК 2.5)	Организует учёт, обработку, хранение и передачу информации ограниченного доступа с соблюдением режима конфиденциальности.	Соблюдает режим конфиденциальности с отдельными недочётами.	Соблюдает режим конфиденциальности частично.	Режим конфиденциальности и нарушен.
Регистрация событий и выявление инцидентов (ПК 2.6)	Работает с подсистемами регистрации событий, выявляет события и инциденты безопасности в АС.	Выявляет события ИБ, но не все инциденты классифицированы.	Фиксирует события без анализа инцидентов.	Регистрация событий и выявление инцидентов не ведутся.
Безопасная разработка и тестирование на проникновение (ПК 2.7д)	Применяет методологии безопасной разработки ПО и проектирования защищённых архитектур, работает с инструментами тестирования на проникновение, анализа уязвимостей и сканирования.	Применяет инструменты анализа уязвимостей, но методология неполная.	Использует отдельные инструменты сканирования без системного анализа.	Методологии безопасной разработки и тестирования на проникновение не применяются.
Защита от социальной инженерии (ПК 2.8д)	Применяет технические и организационные меры защиты от социальной инженерии, моделирует атаки для проверки уровня защищённости организации.	Применяет меры защиты от социальной инженерии без моделирования атак.	Знает меры защиты, но применяет их фрагментарно.	Меры защиты от социальной инженерии не применяются.
Выбор способов решения профессиональных задач (ОК 01)	Обоснованно выбирает способы решения задач профессиональной деятельности применительно к различным контекстам.	Выбирает способ решения задачи, но обоснование неполное.	Выбирает решение шаблонно, без учёта контекста.	Не способен выбрать адекватный способ решения задачи.

Поиск, анализ и интерпретация информации (ОК 02)	Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для решения профессиональных задач.	Использует средства поиска и анализа информации, но анализ упрощён.	Применяет базовые средства поиска; анализ поверхностный.	Современные средства поиска и анализа информации не применяет.
Взаимодействие в коллективе и команде (ОК 04)	Эффективно взаимодействует и работает в коллективе и команде, координирует действия участников.	Взаимодействует в команде, но координация неполная.	Участствует в командной работе пассивно.	Не взаимодействует в коллективе и команде.

**Контрольно-оценочные средства по УП и ПП.03 Защита информации техническими средствами разработаны в соответствии с
ФГОС 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Комплект контрольно-оценочных средств (КОС) практик разработан на основе:

- Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- программы учебной и производственной практик УП и ПП.03 Защита информации.

Комплект контрольно-оценочных средств предназначен для оценки результатов освоения УП и ПП.03 Защита информации.

Результатом освоения практик является готовность обучающегося к выполнению вида профессиональной деятельности «Защита информации техническими средствами» и формирование практического опыта, умений, знаний, профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ОПОП в целом.

В результате освоения дисциплины студент овладеет:

Код ОК и ПК	Умения	Знания
ОК 01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы.	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации.
ОК 04	организовывать работу коллектива и команды взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива психологические особенности личности
ПК 3.1	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.	порядок технического обслуживания технических средств защиты информации; номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам.

ПК 3.2	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами.	физические основы, структура и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности; классификация существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.3	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.	номенклатура и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структура и условия формирования технических каналов утечки информации.
ПК 3.4	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.	номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.5	применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации.	основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатура применяемых средств физической защиты объектов информатизации.
ПК 3.6д	планировать и организовывать проведение тестирования на проникновение в соответствии с поставленными целями; обнаруживать и анализировать уязвимости информационных систем.	основные понятия и методологии тестирования на проникновение; виды тестирования: чёрный ящик, серый ящик, белый ящик; этапы тестирования на проникновение: рекогносцировка, сканирование, эксплуатация, установление доступа, эскалация привилегий, очистка следов, анализ.
ПК 3.7д	анализировать нормативно-правовые акты и адаптировать их требования к специфике деятельности организации; разрабатывать внутренние документы по информационной безопасности: политики, положения, регламенты, инструкции, анкеты, формы договоров.	основные нормативно-правовые акты РФ в сфере информационной безопасности; структура и состав локальных нормативных актов (ЛНА) в области информационной безопасности.
ПК 3.8д	выполнять монтаж, конфигурирование, проверку работоспособности и регламентное техническое обслуживание технических средств защиты информации с соблюдением требований эксплуатационной и технической документации	устройство, принципы действия, технические характеристики и требования эксплуатационной документации к техническим средствам защиты информации, а также регламенты их монтажа, настройка и техническое обслуживание
ПК 3.9д	оценивать уязвимости объектов информации к физическим воздействиям и выбирать оптимальные способы защиты с учётом конструктивных	принципы и методы физической защиты объектов информатизации, характеристик технических средств, видов и параметров дестабилизирующих внешних воздействий,

	особенностей оборудования и условий эксплуатации	а также требования нормативных документов по организации физической безопасности
--	--	--

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной и производственной практик должен:

Иметь опыт:

- установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации
- применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации
- проведение 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
- проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации
- установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты
- использования специализированных инструментов и фреймворков для тестирования безопасности ИС; работы в условиях ограниченного доступа к информации о тестируемой системе
- оформления нормативной и технической документации в соответствии с установленными стандартами делопроизводства и внутренними правилами организации; работы с документооборотом: регистрация, учет, хранение, рассылка, контроль исполнения
- установки, пуска и наладки и сопровождения технических средств защиты информации (СЗИ от НСД, межсетевые экраны, средства криптографической защиты) в составе защищённых информационных систем
- организации физической защиты информационных объектов: размещение и крепление технических средств, применение средств сигнализации, контроля доступа и защиты от дестабилизирующих факторов (вибрация, электромагнитные помехи, климатические воздействия)

Типовые вопросы для оценки результатов учебной и производственной практики

Раздел 1. Вопросы по профессиональным компетенциям (ПК)

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

1. Опишите процесс монтажа и первоначальной настройки технического средства защиты (например, устройства защиты от ПЭМИ, защищённого рабочего места, HSM).
2. Какие требования эксплуатационной документации и нормативных актов (ФСТЭК, ГОСТ) вы учитывали при установке?

3. Пр продемонстрируйте акт ввода в эксплуатацию или протокол технического обслуживания, составленный вами.

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

4. Как вы организовывали режим эксплуатации ТСЗИ (периодичность проверок, обновления, резервирование)?
5. Опишите процедуру контроля работоспособности ТСЗИ в течение практики.
6. Какие нарушения эксплуатационного режима вы выявили и как их устранили?

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

7. Какое оборудование вы использовали для измерения ПЭМИ (анализатор спектра, измерительная антенна и др.)?
8. Опишите методику проведения измерений в соответствии с ГОСТ Р 50922 или ГОСТ Р 51584.
9. Пр продемонстрируйте протокол измерений с выводами о соответствии/несоответствии нормативам.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

10. Как вы измеряли уровень фоновых шумов и физических полей (магнитных, электрических) в защищаемом помещении?
11. Какие нормативные значения вы использовали для сравнения и оценки?
12. Какие рекомендации по снижению излучений вы предложили на основе измерений?

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации

13. Какие меры физической защиты вы реализовали (контроль доступа, видеонаблюдение, сигнализация, экранирование)?
14. Опишите организацию зон безопасности (например, зона ПЭВМ, серверная) в рамках практики.
15. Как вы обеспечивали соответствие требованиям к защищённым помещениям?

ПК 3.6д. Осуществлять тестирование информационной системы на проникновение

16. Опишите смоделированный или реальный пентест: цели, методы, использованные инструменты (Nmap, Burp Suite, Metasploit и др.).
17. Какие уязвимости вы выявили и как они связаны с техническими средствами защиты?
18. Пр продемонстрируйте отчёт по результатам тестирования с рекомендациями по устранению.

ПК 3.7д. Разрабатывать и вести документацию для обеспечения информационной безопасности организации на основе нормативных правовых актов РФ

19. Какие документы ИБ вы разработали (политика ИБ, инструкции, акты, журналы)?
20. Как вы обеспечивали соответствие документации требованиям Ф3-152, Ф3-187, приказам ФСТЭК?
21. Пр продемонстрируйте пример документа с ссылками на нормативные акты.

ПК 3.8д. Осуществлять установку, монтаж, настройку, эксплуатацию и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации

22. Опишите выполненные вами монтаж, настройку и регламентное техническое обслуживание технического средства защиты информации.
23. Как вы проверяли работоспособность технического средства защиты информации после установки и в процессе эксплуатации?

24. Продемонстрируйте эксплуатационный журнал или протокол технического обслуживания технического средства защиты информации, оформленный вами.

ПК 3.9д. Осуществлять физическую защиту объектов информации, в т.ч. учитывая физические характеристики приборов и внешних воздействий

25. Какие меры физической защиты объектов информатизации вы реализовали в ходе практики?
26. Как вы учитывали физические характеристики приборов и возможные внешние воздействия при организации физической защиты?
27. Продемонстрируйте схему или план размещения средств физической защиты объекта информатизации.

Раздел 2. Вопросы по общим компетенциям (ОК)

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

22. Опишите ситуацию выбора между несколькими техническими средствами защиты (например, экранирование vs. шумогенератор). Обоснуйте ваш выбор.
23. Как вы учитывали специфику объекта (офис, дата-центр, мобильное рабочее место) при принятии решений?

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

24. Какие специализированные инструменты и программные комплексы вы использовали (спектроанализаторы, ПО для пентеста, системы мониторинга)?
25. Приведите пример анализа профессиональной литературы или методических рекомендаций на иностранном языке (например, NIST, ISO).

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

26. Опишите вашу роль в командной работе при выполнении комплексного задания (например, проверка защищённости помещения).
27. Как вы координировали действия с инженерами, ИТ-специалистами или наставником?

Раздел 3. Комплексные практические задания

Для учебной практики:

32. Установите и настройте техническое средство защиты информации (например, устройство защиты от ПЭМИ или защищённую рабочую станцию) в лабораторных условиях.
33. Проведите измерения ПЭМИ и фоновых шумов, оформите протокол в соответствии с требованиями ГОСТ.
34. Разработайте комплект локальной документации по ИБ для учебного класса (инструкция по работе с ТСЗИ, журнал учёта, политика доступа).

Для производственной практики:

35. Организуйте и проведите комплексную проверку технической защищённости рабочего места с информацией ограниченного доступа.
36. Выполните тестирование на проникновение в ИС с последующим анализом эффективности технических средств защиты.
37. Разработайте и внедрите меры физической и технической защиты для реального объекта информатизации в соответствии с требованиями ФСТЭК.

Критерии оценки:

Критерий	5	4	3	2
Монтаж и техобслуживание технических СЗИ (ПК 3.1)	Выполняет установку, монтаж, настройку и техническое обслуживание технических средств защиты информации; применяет их основные типы.	Выполняет монтаж и ТО технических СЗИ с отдельными недочётами.	Выполняет базовые операции монтажа формально.	Монтаж и ТО технических СЗИ не выполнены или с грубыми нарушениями.
Применение ТСЗИ и выявление ТКУИ (ПК 3.2)	Применяет технические средства защиты, выявляет технические каналы утечки информации, участвует в мониторинге эффективности, диагностирует и устраняет отказы ТСЗИ.	Применяет ТСЗИ и выявляет ТКУИ, но мониторинг неполный.	Выявляет отдельные каналы утечки без диагностики.	Технические каналы утечки не выявляются; ТСЗИ применяются неверно.
Измерения параметров ПЭМИН (ПК 3.3)	Проводит измерения параметров ПЭМИН, создаваемых техническими средствами обработки информации, при аттестации объектов информатизации по требованиям безопасности информации.	Проводит измерения ПЭМИН, но методика с отдельными отклонениями.	Измерения ПЭМИН фрагментарны; анализ ограничен.	Измерения ПЭМИН не проведены или выполнены неверно.
Измерения фоновых шумов и физических полей (ПК 3.4)	Проводит измерения параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты; выявляет технические каналы утечки информации.	Проводит измерения полей с отдельными недочётами.	Измерения выполнены частично.	Измерения не проведены.
Инженерно-технические средства физической защиты (ПК 3.5)	Выполняет монтаж, настройку, техническое обслуживание, диагностику и восстановление работоспособности инженерно-технических средств физической защиты.	Обслуживает средства физической защиты с отдельными недочётами.	Выполняет базовые операции без диагностики.	Средства физической защиты не обслуживаются.
Тестирование безопасности ИС (ПК 3.6д)	Использует специализированные инструменты и фреймворки для тестирования безопасности ИС, в том числе в условиях ограниченного доступа к информации о системе.	Использует инструменты тестирования, но ограниченно.	Применяет отдельные инструменты без системного подхода.	Тестирование безопасности не проводится.
Документация и документооборот ИБ (ПК 3.7д)	Оформляет нормативную и техническую документацию в соответствии со стандартами делопроизводства; ведёт документооборот (регистрация, учёт, хранение, рассылка, контроль исполнения).	Оформляет документацию с отдельными нарушениями стандартов.	Документация неполная или неформатная.	Документация не оформлена.
Пусконаладка и сопровождение технических СЗИ (ПК 3.8д)	Выполняет установку, пусконаладку и сопровождение технических средств защиты информации (СЗИ от НСД, межсетевые экраны, СКЗИ) в составе защищённых информационных систем.	Выполняет пусконаладку технических СЗИ с отдельными недочётами.	Выполняет установку без полной пусконаладки.	Пусконаладка и сопровождение не выполнены.

Физическая защита информационных объектов (ПК 3.9д)	Организует физическую защиту информационных объектов: размещает и крепит технические средства, применяет средства сигнализации, контроля доступа и защиты от дестабилизирующих факторов.	Организует физическую защиту, но задействованы не все средства.	Обеспечивает физическую защиту частично.	Физическая защита не организована.
Выбор способов решения профессиональных задач (ОК 01)	Обоснованно выбирает способы решения задач профессиональной деятельности применительно к различным контекстам.	Выбирает способ решения задачи, но обоснование неполное.	Выбирает решение шаблонно, без учёта контекста.	Не способен выбрать адекватный способ решения задачи.
Поиск, анализ и интерпретация информации (ОК 02)	Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для решения профессиональных задач.	Использует средства поиска и анализа информации, но анализ упрощён.	Применяет базовые средства поиска; анализ поверхностный.	Современные средства поиска и анализа информации не применяет.
Взаимодействие в коллективе и команде (ОК 04)	Эффективно взаимодействует и работает в коллективе и команде, координирует действия участников.	Взаимодействует в команде, но координация неполная.	Участвует в командной работе пассивно.	Не взаимодействует в коллективе и команде.

Контрольно-оценочные средства по УП и ПП.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин) разработаны в соответствии с
ФГОС 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Комплект контрольно-оценочных средств (КОС) практик разработан на основе:

- Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- программы учебной и производственной практик УП и ПП.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин).

Комплект контрольно-оценочных средств предназначен для оценки результатов освоения УП и ПП. 04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин).

Результатом освоения практик является готовность обучающегося к выполнению вида профессиональной деятельности «Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин)» и формирование практического опыта, умений, знаний, профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ОПОП в целом.

В результате освоения дисциплины студент овладеет:

Код ОК и ПК	Умения	Знания
ОК 01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы.	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации.
ОК 04	организовывать работу коллектива и команды взаимодействовать с коллегами,	психологические основы деятельности коллектива психологические

	руководством, клиентами в ходе профессиональной деятельности	особенности личности
ПК 4.1д	выполнять требования техники безопасности при работе с вычислительной техникой; производить подключение блоков персонального компьютера и периферийных устройств; производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; выполнять инсталляцию системного и прикладного программного обеспечения.	требования техники безопасности при работе с вычислительной техникой; основные принципы устройства и работы компьютерных систем и периферийных устройств.
ПК 4.2д	создавать и управлять содержимым документов с помощью текстовых процессоров; создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; создавать и управлять содержимым презентаций с помощью редакторов презентаций; использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных; эффективно пользоваться запросами базы данных; создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики, производить сканирование документов и их распознавание; производить распечатку, копирование и тиражирование документов на принтере и других устройствах.	программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета.
ПК 4.3д	управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете; осуществлять навигацию по веб-ресурсам Интернета с помощью браузера, осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет-сайтов.	классификация и назначение компьютерных сетей, виды носителей информации.
ПК 4.4д	осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; осуществлять резервное копирование и восстановление данных.	основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения учебной и производственной практик должен:

Иметь опыт:

- устанавливать, настраивать и обслуживать программное обеспечение компьютерной системы, управлять файлами, применять офисное программное обеспечение в соответствии с прикладной задачей
- производить работу с текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах

- использовать ресурсы, технологии и сервисы интернет; использовать ресурсы локальной вычислительной сети
- применять средства защиты информации в компьютерной системе

Типовые вопросы для оценки результатов учебной и производственной практики

Раздел 1. Вопросы по профессиональным компетенциям (ПК)

ПК 4.1д. Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения

1. Опишите процесс подготовки рабочего места оператора ЭВМ: от распаковки оборудования до запуска операционной системы.
2. Какие этапы включала установка и настройка программного обеспечения (ОС, офисные приложения, антивирус, средства ИБ)?
3. Продемонстрируйте скрипт или последовательность действий по автоматизации развёртывания ПО и обоснуйте выбор метода.

ПК 4.2д. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах

4. Продемонстрируйте созданный вами текстовый документ, таблицу и презентацию в соответствии с требованиями делопроизводства.
5. Как вы организовали структуру базы данных (например, в Access или LibreOffice Base) и какие запросы реализовали?
6. Приведите пример работы в графическом редакторе (создание схемы, оформление отчёта, обработка изображений).

ПК 4.3д. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

7. Как вы подключались к локальной сети и использовали сетевые ресурсы (принтеры, общие папки, серверы)?
8. Опишите процесс поиска, анализа и использования информации из интернета для решения профессиональной задачи.
9. Какие облачные сервисы (Google Workspace, Яндекс.Диск, MS 365) вы применяли и для каких целей?

ПК 4.4д. Обеспечивать применение средств защиты информации в компьютерной системе

10. Какие средства защиты информации вы настроили на рабочей станции (антивирус, брандмауэр, политики безопасности, шифрование)?
11. Как вы обеспечивали защиту персональных данных при работе с документами и базами данных?
12. Продемонстрируйте настройку политик доступа, резервного копирования и аудита на уровне пользователя.

Раздел 2. Вопросы по общим компетенциям (ОК)

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

13. Опишите ситуацию, когда вам пришлось выбирать между разными способами установки ПО (локально vs. через сеть, open-source vs. коммерческое). Обоснуйте ваш выбор.
14. Как вы адаптировали свои действия при работе с разными типами пользователей (администратор, бухгалтер, руководитель)?

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

15. Какие цифровые инструменты вы использовали для повышения эффективности работы (менеджеры задач, автоматизация, макросы)?

16. Приведите пример поиска и применения решения технической проблемы с использованием профессиональных ресурсов (официальная документация, форумы, видеоуроки).
- ОК 04. Эффективно взаимодействовать и работать в коллективе и команде
17. Опишите ваш вклад в совместную работу (например, настройка общего сетевого пространства, подготовка материалов для команды).
18. Как вы координировали действия с коллегами при решении общей задачи (например, миграция данных, обновление ПО)?

Раздел 3. Комплексные практические задания

Для учебной практики:

23. Подготовьте рабочее место оператора ЭВМ: соберите ПК (виртуально или физически), установите ОС, настройте ПО, подключите к локальной сети.
24. Создайте комплексный документационный пакет: отчёт в Word, аналитическую таблицу в Excel, презентацию в PowerPoint и простую БД в Access.
25. Настройте средства защиты информации на рабочей станции и продемонстрируйте их работу (резервное копирование, шифрование, антивирусная проверка).

Для производственной практики:

26. Выполните полный цикл обслуживания рабочего места сотрудника: диагностика, обновление ПО, настройка сетевых ресурсов, обучение пользователя.
27. Организуйте и внедрите систему хранения и обмена документами в команде с использованием локальных и облачных ресурсов.
28. Проведите аудит ИБ рабочих станций подразделения и предложите меры по усилению защиты (обновление политик, настройка DLP, обучение).

Критерии оценки:

Критерий	5 (Отлично)	4 (Хорошо)	3 (Удовлетворительно)	2 (Неудовлетворительно)
Инсталляция и обслуживание ПО (ПК 4.1д)	Инсталлирует, настраивает и обслуживает программное обеспечение компьютерной системы, управляет файлами, применяет офисное ПО в соответствии с прикладной задачей.	Инсталлирует и обслуживает ПО с отдельными недочётами.	Выполняет базовую установку ПО без оптимизации.	ПО не инсталлировано или настроено неверно.
Работа с документами, данными и графикой (ПК 4.2д)	Работает с текстовыми документами, таблицами, презентациями и содержанием баз данных, использует графические редакторы в соответствии с требованиями.	Работает с документами и данными; графика или БД выполнены упрощённо.	Создаёт документы формально, с ошибками оформления.	Задание с документами и данными не выполнено.
Использование сетевых и интернет-ресурсов (ПК 4.3д)	Использует ресурсы, технологии и сервисы Интернета, а также ресурсы локальной вычислительной сети для решения задач.	Использует сетевые и интернет-ресурсы с отдельными недочётами.	Использует базовые сетевые ресурсы ограниченно.	Сетевые и интернет-ресурсы не используются.
Применение средств защиты информации (ПК 4.4д)	Применяет средства защиты информации в компьютерной системе в соответствии с требованиями ИБ.	Применяет средства защиты с отдельными недочётами.	Применяет базовые средства защиты фрагментарно.	Средства защиты информации не применяются.
Выбор способов решения профессиональных задач (ОК 01)	Обоснованно выбирает способы решения задач профессиональной деятельности	Выбирает способ решения задачи, но обоснование неполное.	Выбирает решение шаблонно, без учёта контекста.	Не способен выбрать адекватный способ решения задачи.

	применительно к различным контекстам.			
Поиск, анализ и интерпретация информации (ОК 02)	Использует современные средства поиска, анализа и интерпретации информации и информационные технологии для решения профессиональных задач.	Использует средства поиска и анализа информации, но анализ упрощён.	Применяет базовые средства поиска; анализ поверхностный.	Современные средства поиска и анализа информации не применяет.
Взаимодействие в коллективе и команде (ОК 04)	Эффективно взаимодействует и работает в коллективе и команде, координирует действия участников.	Взаимодействует в команде, но координация неполная.	Участствует в командной работе пассивно.	Не взаимодействует в коллективе и команде.