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

Комплект контрольно-оценочных средств

по практике

УП.02 Учебная практика

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2023

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Составитель:

Гадяцкая И.Д., преподаватель ОГАПОУ «Алексеевский колледж»

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу УП.02 Учебная практика.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы УП.02 Учебная практика.

1.2 Цели и задачи практики – требования к результатам освоения рабочей программы практики:

Практика является обязательным разделом образовательной программы. Она представляет собой вид учебной деятельности в форме практической подготовки, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

С целью овладения видом деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующими профессиональными компетенциями обучающийся в ходе освоения программы учебной практики должен

иметь практический 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.

уметь:

У1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У 2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У4 применять программные и программно-аппаратные средства для защиты информации в базах данных;

У5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У6 применять математический аппарат для выполнения криптографических преобразований;

У7 использовать типовые программные криптографические средства, в том числе электронную подпись;

У8 применять средства гарантированного уничтожения информации;

У9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

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

знать:

З1 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З2 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З3 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З4 основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З5 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З6 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Перечень знаний, умений, навыков в соответствии со спецификацией чемпионатного движения по профессиональному мастерству «Профессионалы» компетенции Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:

1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;

2) знать и понимать: каналы передачи данных: определение и виды;

3) знать и понимать: технологии работы с политиками информационной безопасности;

4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;

5) уметь: администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;

6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

Планируемые личностные результаты освоения рабочей программы

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.

Результатом освоения рабочей программы практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках профессионального модуля ПМ.03 Защита информации техническими средствами по основному виду деятельности - Защита информации техническими средствами, в том числе профессиональными компетенциями (ПК):

Код	Наименование компетенции
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.

1.3 Результаты освоения учебной практики, подлежащие проверке

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения в рамках текущей аттестации (номер задания)	Средства контроля и оценки результатов обучения в рамках промежуточной аттестации (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1. Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ОК 1-11 ПК 2.1-2.6 ЛР 4,7,9,10,11	ПЗ №1-53	КВ №1-18 ТЗ №1-20

2. Комплект оценочных средств для промежуточной аттестации

2.1. Контрольные вопросы

КВ 1. Концепция информационной безопасности.

КВ 2. Каналы утечки информации.

КВ 3. Виды ПО. Назначение и функции ОС.

КВ 4. Классификация операционных систем.

КВ 5. Локальные и удаленные атаки и методы взлома ОС.

КВ 6. Защита от локального НСД.

КВ 7. Протокол Kerberos.

КВ 8. Протокол S/key

КВ 9. Идентификация и аутентификация.

КВ 10.Подсистема аутентификации Windows.

КВ 11. Разграничение доступа.

КВ 12. Избирательный и мандатный метод разграничения доступа.

КВ 13. Аудит.

КВ 14. Политика аудита.

КВ 15. Фрагментарный и комплексный подход к построению ОС.

КВ 16. Методы анализа сетевой информации.

КВ 17. Защищенность БД

КВ 18. Модели безопасности БД

2.2. Тестовые задания (ТЗ)

Тестовое задание	Вариант ответа
1. Защита информации это-	А) потенциальная возможность неправомерного преднамеренного или случайного воздействия, приводящее к потере или разглашению информации. Б) реализация права на государственную тайну и конфиденциальную информацию В) устранение или нейтрализация негативных источников, причин и условий воздействия на информацию **Г) правовые, организационные и технические меры, направленные на обеспечение защиты информации**
2. Каналы утечки информации - это	А) это комплексы специального

	технического и программного обеспечения, предназначенные для предотвращения утечки информации **Б) методы и пути утечки информации из информационной системы** В) потенциальная возможность неправомерного преднамеренного или случайного воздействия Г) соблюдение конфиденциальности информации ограниченного доступа
3. Существуют следующие виды ПО (добавьте недостающее).	А) Прикладное ПО Б) Системное ПО В) **Инструментальное ПО**
4. К функциям ОС относится :	А) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой **Б) управление процессором путем чередования выполнения программ;** В)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы; **Г)управление памятью путем выделения программам на время их выполнения требуемой памяти;**
5. Операционная система Windows является :	**А) многозадачной** Б) однозадачной **В) многопользовательской** Г) однопользовательской
6. Атаки на ОС бывают:	**А) Локальными** Б) Глобальными **В) Удаленными** Г) Близкими
7. Профессиональный взлом имеет следующую структуру (восстановите последовательность)	А) попытка внедрения вредоносных программ Б) поиск уязвимостей в ПО ЗИ В) тщательный анализ ПО Г) анализ выбранной политики безопасности **Ответ Г,В,Б,А**
8. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:	**А) парольная аутентификация** Б) аутентификация по магнитному носителю В) модель рукопожатия Г) аутентификация по характеристикам работы

	пользователя
9. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:	А) парольная аутентификация **Б) аутентификация по магнитному носителю** В) модель рукопожатия Г) аутентификация по характеристикам работы пользователя
10. К защите от удаленного НСД можно отнести:	**А) модель рукопожатия** **Б) Протокол Kerberos** В) Аутентификация по биометрическим характеристикам Г) Аутентификация по росписи мышью
11. Целью защиты информации является:	А) предотвращение хищения, утечки, искажения, утраты и подделки информации; **Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;** В) реализация права на государственную тайну и конфиденциальную информацию Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации
12. К основным видам средств защиты информации относится:	**А) нормативно-правовые** **Б) Технические** В) Экологические Г) Этнические
13. Технические средства защиты – это	А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации **Б) это комплексы специального технического и программного обеспечения** В) правила и нормы поведения, направленные на обеспечение безопасности информации Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе

14. К каналам утечки информации относится:	**А) Магнитный канал** **Б) Виброакустический канал** **В) Лазерный канал** Г) Специальный канал
15. К назначению ОС относится:	А)управление процессором путем чередования выполнения программ; Б)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы; В)управление памятью путем выделения программам на время их выполнения требуемой памяти; **Г)поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;**
16. Многопроцессорная обработка в ОС бывает:	**А) Симметричной** Б) Квадратичной В) Полной **Г) Ассиметричной**
17. К локальной защите от НСД относится:	**А) Аутентификация на основе биометрических характеристик** Б) Протокол CHAP **В) Парольная аутентификация** Г) Проток PAP
18. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:	А) парольная аутентификация Б) аутентификация по магнитному носителю В) модель рукопожатия **Г) аутентификация по характеристикам работы пользователя**
19. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.	А) PAP Б) CHAP **В) S/KEY** Г) Kerberos
20. К недостаткам дискреционного управления доступом относится:	**А) нельзя контролировать утечку конфиденциальной информации** Б) неудобство для пользователя В) нет опасности утечки конфиденциальной информации Г) слабая защита от вредоносных программ

3. Критерии оценивания

«5» «отлично»– студент показывает глубокое и полное овладение содержанием программного материала по МДК, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо»– студент в полном объеме освоил программный материал по МДК, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно»– студент обнаруживает знание и понимание основных положений программного материала по МДК, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

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. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с

2. 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.

Дополнительные источники:

1.Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.

2.Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.

3.Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4.Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.

5.Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

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:

- Абрамов, Г. В. Проектирование и разработка информационных систем : учебное пособие для СПО / Г. В. Абрамов, И. Е. Медведкова, Л. А. Коробова. — Саратов : Профобразование, 2020. — 169 с. — ISBN 978-5-4488-0730-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/88888 (дата обращения: 07.09.2020). — 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/