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

Комплект контрольно-оценочных средств

по учебной дисциплине

ОП 19. Безопасность информационных систем

для специальности
09.02.07
Информационные системы и программирование

Алексеевка – 2023

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1547, с учетом профессионального стандарта «Администратор баз данных», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 17 сентября 2014 года № 647н.

Составитель:
Рогачева О. Н., 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 учебной дисциплины ОП 19. Безопасность информационных систем.

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

КОС разработан на основании рабочей программы учебной дисциплины ОП 19. Безопасность информационных систем.

1.2 Цели и задачи учебной дисциплины **– требования к результатам освоения программы:**

В результате освоения учебной дисциплины обучающийся должен **уметь**:

У1 ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;

У2 анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;

У3 применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.

В результате освоения учебной дисциплины обучающийся должен **знать**:

З1объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;

З2понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;

З3базовые составляющие в области развития систем информационной безопасности;

З4классификацию объектов защиты.

Профессиональные (ПК) и общие (ОК) **компетенции**, которые актуализируются при изучении учебной дисциплины:

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

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

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях

ОК 04 Эффективно взаимодействовать и работать в коллективе и команде

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

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

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

ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием

ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания

ПК 7.2. Осуществлять администрирование отдельных компонент серверов

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации

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

1) знать и понимать:

- понимание принципов работы специалиста по информационной безопасности и их применение;
- знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;
- регламентирующие документы в области безопасности информационных систем;
- регламентирующие документы в области охраны труда и безопасности жизнедеятельности;
- важность организации труда в соответствии с методиками;
- методы и технологии исследования;
- важность управления собственным профессиональным развитием;
- скорость изменения Ит-сферы и области информационной

безопасности, а также важность соответствия современному уровню.

- важность умения слушать собеседника как части эффективной коммуникации;
- роли и требования коллег и наиболее эффективные методы коммуникации; • важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими;
- способы разрешения непонимания и конфликтующих требований;

2) уметь:

- интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;
- применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;
- настраивать сетевые устройства;
- администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;
- установка агентской части системы корпоративной защиты от внутренних угроз;
- запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров;
- настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом;
- уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки;

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

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

1.3 Результаты освоения учебной дисциплины, подлежащие проверке

Наименование тем	Коды умений (У), знаний (З), личностных результатов (ЛР), 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. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	У1-У3 З1-З4 ЛР 4 ЛР 7	ПЗ №1	ПЗ №1 КВ №1-16
Тема 2. Исследование (аудит) организации с целью защиты от внутренних угроз	У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №2	ПЗ №1 КВ №1-16
Тема 3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	У1-У3 З1-З4 ЛР 4	ПЗ №3	ПЗ №1 КВ №1-16
Тема 4. Технологии анализа и защиты сетевого трафика	У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №4	ПЗ №1 КВ №1-16
Тема 5. Технологии агентского мониторинга	У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №5	ПЗ №1 КВ №1-16
Тема 6. Анализ выявленных инцидентов	У1-У3 З1-З4 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №6	ПЗ №1 КВ №1-16

2. Комплект оценочных средств для текущей аттестации

2.1. Практические задания (ПЗ)

ПЗ №1 УСТАНОВКА, КОНФИГУРИРОВАНИЕ И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ В СИСТЕМЕ КОРПОРАТИВНОЙ ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ

Задания для выполнения практической работы:

1. Провести конфигурацию сетевой инфраструктуры: настроить хост-машину, сетевое окружение, виртуальные машины, и т.п.;
2. Установить и настроить систему корпоративной защиты от внутренних угроз;
3. Запустить систему, проверить функциональность и соответствие настроек целевой сетевой инфраструктуре
4. Провести имитацию процесса утечки конфиденциальной информации в системе; -
5. Устранить проблемы при появлении;
6. Продемонстрировать работоспособность системы
7. Подготовить отчёт по оценке работоспособности системы;

ПЗ №2 ИССЛЕДОВАНИЕ (АУДИТ) ОРГАНИЗАЦИИ С ЦЕЛЬЮ ЗАЩИТЫ ОТ ВНУТРЕННИХ УГРОЗ

Задания для выполнения практической работы:

1. провести обследование и анализ структуры организации (как главного объекта защиты) на основании представленных материалов и стенда, её вычислительно-сетевой инфраструктуры, определить потоки данных, потенциальные угрозы и каналы утечек.
2. создать пакет документации, включающий

- список потенциальных внутренних угроз (согласно выданного шаблона)
- список возможных каналов связи для анализа (согласно выданного шаблона)
- проект положения о защите информации от внутренних угроз (согласно выданного шаблона)
- список ролей пользователей и потенциальных нарушителей - список изменений в существующие внутренние нормативных документы (положения, приказы и т.п.) организации для эффективного и законного использования современных систем защиты.

3. Подготовить отчёт, суммирующий итоги исследования организации.

ПЗ №3 РАЗРАБОТКА ПОЛИТИК БЕЗОПАСНОСТИ В СИСТЕМЕ КОРПОРАТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ.

Задания для выполнения практической работы:

1. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты;
2. Занести политики информационной безопасности в DLP-систему;
   Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;

3. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;

4. Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM.

ПЗ №4 ТЕХНОЛОГИИ АНАЛИЗА И ЗАЩИТЫ СЕТЕВОГО ТРАФИКА.

Задания для выполнения практической работы:

1. Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.
2. Администрирование узлов и пользователей.
3. Выполнение компрометации узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации.
4. Организацию межсетевого взаимодействия и туннелированния.
5. Внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

ПЗ №5 ПОИСК И ПРЕДОТВРАЩЕНИЕ ИНЦИДЕНТОВ. ТЕХНОЛОГИИ АНАЛИЗА СЕТЕВОГО ТРАФИКА В СИСТЕМЕ КОРПОРАТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВНУТРЕННИХ УГРОЗ

Задания для выполнения практической работы:

1. Продемонстрировать знание механизмов работы агентского мониторинга;
2. Разработать и применить политики агентского мониторинга для работы с носителями и устройствами;
3. Разработать и применить политики агентского мониторинга для работы с файлами;
4. Работа с исключениями из перехвата;

ПЗ №6 АНАЛИЗ ВЫЯВЛЕННЫХ ИНЦИДЕНТОВ

Задания для выполнения практической работы:

1. Применить механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
2. Подготовить детализированные отчёты о нарушениях;
3. Провести классификацию уровня угрозы инцидента;
4. Использовать дополнительных модули анализа информационных потоков, если это продиктовано особенностями модели организации и условиями её бизнеса;
5. Разработать план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу;

6. Подготовить итоговый отчёт

3. Комплект оценочных средств для промежуточной аттестации

3.1. Практические задания (ПЗ)

ПЗ №1

Цель разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для выявления и/или блокирования инцидентов безопасности. Для создания инцидентов и других событий в IWTM используется специальное программное обеспечение – специальный Генератор трафика и инцидентов. Участнику необходимо:

1. Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;
2. Занести политики информационной безопасности в DLP-систему;
3. Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;
4. Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;
5. Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM. Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов). Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. Итоговый вариант политик должен быть зафиксированы в отчете. В число инцидентов могут входить, например:

– передача персональных данных сотрудников и контрагентов по электронной почте;

– передача базы клиентов организации в архиве с использованием файловых протоколов;

– нецензурная лексика сотрудников в переписке с контрагентами;

– передача информации, составляющей коммерческую тайну и др.

Задание выполняется с помощью программного обеспечения DLP (Data Leaks Prevention) IWTM 6.

3.2. Контрольные вопросы (КВ)

КВ№1 Технологии работы с политиками информационной безопасности.

КВ№2 Создание новых политик, модификация существующих.

КВ№3 Общие принципы при работе интерфейсом системы защиты корпоративной информации.
КВ№4 Объекты защиты, персоны.
КВ№5 Ключевые технологии анализа трафика.
КВ№6 Типовые протоколы и потоки данных в корпоративной среде,
КВ№7 Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек.
КВ№8 Типы угроз информационной безопасности, типы инцидентов,
КВ№9 9. Технологий анализа трафика при работе с политиками информационной безопасности в системе корпоративной защиты информации.
КВ№10 Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации.
КВ№11 Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных.
КВ№12 12. Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации.
КВ№13 Роль фильтров при анализе перехваченного трафика. Технические ограничения механизма фильтрации, его преимущества и недостатки.
КВ№14 14. Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе.
КВ№15 Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов.
КВ№16 Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации.

4. Критерии оценивания

«5» «отлично» или «зачтено» – студент показывает глубокое и полное овладение содержанием программного материала по УД, 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» или «зачтено» – студент в полном объеме освоил программный материал по УД, 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» или «зачтено» – студент обнаруживает знание и понимание основных положений программного материала по УД, 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» или «не зачтено» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по УД, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

5. 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. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. – М.: Академия. 2019-256 с.

Дополнительные источники:

2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
3. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
4. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
5. ГубенковА.А.Информационнаябезопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
6. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
7. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
8. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
9. Мельников Д. Информационная безопасность открытых систем.-М.: Форум, 2013.
10. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.
11. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.
12. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д.А.–М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

Электронные издания (электронные ресурсы)

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Российский биометрический портал www.biometrics.ru
4. Сайт журнала Информационная безопасность http://www.itsec.ru –
5. Справочно-правовая система «Гарант» » www.garant.ru

6. Справочно-правовая система «Консультант Плюс» www.consultant.ru 9. Федеральная служба по техническому и экспортному контролю
7. (ФСТЭК России) www.fstec.ru

Цифровая образовательная среда СПО PROFобразование:

1. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 263 c. — ISBN 978-5-4497-0666-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/97553 (дата обращения: 12.11.2020). — Режим доступа: для авторизир. Пользователей
2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 125 c. — ISBN 978-5-4487-0299-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/77318 (дата обращения: 13.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS

https://www.iprbookshop.ru/89443.html

https://www.iprbookshop.ru/6991.html

Веб-система для организации дистанционного обучения и управления им:

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