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

УТВЕРЖДАЮ:
Заместитель директора
_____И.А. Злобина
31 августа 2021 г.

Комплект контрольно-оценочных средств

по учебной дисциплине

ОП 19. Безопасность информационных систем

для специальности
09.02.07
Информационные системы и программирование

Алексеевка – 2021

РАССМОТРЕНО
на заседании предметно-цикловой комиссии
общепрофессиональных дисциплин и профессиональных модулей
специальностей 09.02.04 Информационные системы (по отраслям) и 09.02.07
Информационные системы и программирование
Протокол № 1 от 31 августа 2021 г.

Председатель _____ И.В. Косинова

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование

Составитель: Рогачева Олеся Николаевна, преподаватель

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 Система контроля и оценки освоения программы учебной дисциплины

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения теоретических и практических занятий, дифференцированного зачета.

Результаты обучения (освоенные умения, усвоенные знания), с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Формы и методы контроля и оценки результатов обучения**
умения: ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности; анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности; применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет
знания: объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности; понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности; базовые составляющие в области развития систем информационной безопасности; классификацию объектов защиты.	Экспертное наблюдение и оценка при выполнении практической работы, проверка домашнего задания. Тестирование, защита практической работы, устный и письменный опрос, дифференцированный зачет

2. Комплект оценочных средств

2.1. Контрольные вопросы к дифференцированному зачету

Технологии работы с политиками информационной безопасности; 2. Создание новых политик, модификация существующих;

3. Общие принципы при работе интерфейсом системы защиты корпоративной информации;

4. Объекты защиты, персоны;

5. Ключевые технологии анализа трафика;

6. Типовые протоколы и потоки данных в корпоративной среде, такими как:корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4), веб-почта; Интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS); социальные сети; интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, Google Talk, Skype, QIP; принтеры: печать файлов на локальных и сетевых принтерах; любые съемные носители иустройства;

7. Осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;

8. Типы угроз информационной безопасности, типы инцидентов,

9. Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

10. Основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;

11. Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

12. Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;

13. Роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;

14. Разделысистемы корпоративной безопасности, которые используются офицером безопасности в повседневной работе;

15. Особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;

16. Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации.

2.2 Оценочные материалы для итоговой аттестации:

Модуль 1: Анализа информационного пространства

Цель участника – 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.

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.

3. 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 с. — 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 с. — 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/