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

Комплект контрольно-оценочных средств

по МДК. 02.01 Программные и программно-аппаратные средства защиты информации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2024

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553, с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н.

Составитель:

Ковалев Н.А., 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 МДК.03.01 Техническая защита информации.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме экзамена.

КОС разработан на основании рабочей программы МДК.02.01. Программные и программно-аппаратные средства защиты информации.

1.2. Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

уметь:

У.1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

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

У.3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У.4 применять программные и программно-аппаратные средства для защиты информации в базах данных;

У.5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У.6 применять математический аппарат для выполнения криптографических преобразований;

У.7 использовать типовые программные криптографические средства, в том числе электронную подпись;

У.8 применять средства гарантированного уничтожения информации;

У.9 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:

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

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

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

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

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

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

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионата «Профессионалы» Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении междисциплинарного курса:

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 МДК является овладение обучающимися видом деятельности - Защита информации в автоматизированных системах

программными и программно-аппаратными средствами, в том числе общие компетенции (ОК) и профессиональными компетенциями (ПК):

Код	Наименование результата обучения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.3 Результаты освоения междисциплинарного курса, 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 1.1. Предмет и задачи программно-аппаратной защиты информации	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9
Тема 1.2. Стандарты безопасности	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №1	ТЗ №1-20 ПЗ №1-9
Тема 1.3. Защищенная автоматизированная система	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №2,3.4	ТЗ №1-20 ПЗ №1-9
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №5	ТЗ №1-20 ПЗ №1-9
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №7	ТЗ №1-20 ПЗ №1-9
Тема 2.1. Основы защиты автономных автоматизированных систем	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9

Тема 2.2.Защита программ от изучения	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9
Тема 2.3. Вредоносное программное обеспечение	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №8-9	ТЗ №1-20 ПЗ №1-9
Тема 2.4. Защита программ и данных от несанкционированного копирования	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №10-11	ТЗ №1-20 ПЗ №1-9
Тема 2.5. Защита информации на машинных носителях	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №12-15	ТЗ №1-20 ПЗ №1-9
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9
Тема 2.7. Системы обнаружения атак и вторжений	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №16	ТЗ №1-20 ПЗ №1-9
Тема 3.1. Основы построения защищенных сетей	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9
Тема 3.2. Средства организации VPN	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №17	ТЗ №1-20 ПЗ №1-9
Тема 4.1.Обеспечение безопасности	ОК1-7 ОК10	ПЗ №18,19	ТЗ №1-20 ПЗ №1-9

межсетевого взаимодействия	ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		
Тема 5.1. Защита информации в базах данных	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №20,21	ТЗ №1-20 ПЗ №1-9
Тема 6.1. Мониторинг систем защиты	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №22	ТЗ №1-20 ПЗ №1-9
Тема 6.2. Изучение мер защиты информации в информационных системах	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11	ПЗ №23-25	ТЗ №1-20 ПЗ №1-9
Тема 6.3. Изучение современных программно-аппаратных комплексов	ОК1-7 ОК10 ПК 2.1-2.6 З1-З4 У1-У10 ЛР4, ЛР7-11		ТЗ №1-20 ПЗ №1-9

2. Комплект оценочных средств для текущей аттестации

МДК 02.01 Программно–аппаратные средства обеспечения информационной безопасности

2.1. Практические задания (ПЗ)

2.1. Практические задания (ПЗ)

ПЗ №1 Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов

ПЗ №2 Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа.

ПЗ №3 Регистрация событий (аудит). Контроль целостности данных. Уничтожение

остаточной информации.
ПЗ №4 Управление политикой безопасности. Шаблоны безопасности
Криптографическая защита. Обзор программ шифрования данных
Управление политикой безопасности. Шаблоны безопасности
ПЗ №5 Распределение каналов в соответствии с источниками воздействия
ПЗ №6-7 Организация доступа к файлам
Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД
ПЗ №8-9 Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО
ПЗ №10 Защита информации от несанкционированного копирования с использованием специализированных программных средств
ПЗ № 11. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)
ПЗ №12. Применение средства восстановления остаточной информации на примере Foremost или аналога
ПЗ №13. Применение специализированного программно средства для восстановления удаленных файлов
ПЗ №14. Применение программ для безвозвратного удаления данных
ПЗ №15. Применение программ для шифрования данных на съемных носителях
ПЗ №16. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений
ПЗ №17 Развертывание VPN
ПЗ №18 Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.
ПЗ № 19. Изучение различных способов закрытия "опасных" портов
ПЗ №20. Изучение механизмов защиты СУБД MS Access
ПЗ № 1. Изучение штатных средств защиты СУБД MSSQL Server.
ПЗ №22. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов
ПЗ № 23. Проведение аудита ЛВС сетевым сканером.
ПЗ №24 Выбор мер защиты информации для их реализации в информационной системе.
ПЗ №25 Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке

3. Комплект оценочных средств для промежуточной аттестации

3.1. Тестовые задания (ТЗ)

Тест на тему «Программно–аппаратные средства обеспечения информационной безопасности»

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой

+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

29) Ценность информации определяется:

- a) степенью ее полезности для владельца
- b) истинностью или достоверностью
- c) конфиденциальностью

30) Объектом защиты информации является:

- a) работа, посвященная защите информации в автоматизированных системах
- b) компьютерная система или автоматизированная система обработки данных
- c) комплекс средств, предназначенных для автоматизированного сбора

31) Компьютерная система- это...

- a) вычислительные комплексы и системы
- b) вычислительные сети
- c) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации

32) Под системой защиты информации в КС понимается:

- a) состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне
- b) одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы
- c) единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

33) Сеть ЭВМ - это...

- a) процессы сбора, обработки, накопления, хранения, поиска и распространения информации
- b) это совокупность ЭВМ, взаимосвязанных каналами передачи данных, и необходимых для реализации этой взаимосвязи программного обеспечения и (или) технических средств, предназначенных для организации распределенной обработки данных
- c) информация, возникающая в ходе ведения разговоров, работы систем связи, звуко - усиления и звуковоспроизведения

34) Под информационной системой понимают:

- a) упорядоченную совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
- b) процессы сбора, обработки, накопления, хранения, поиска и распространения информации
- c) информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче

35) Информационными ресурсами называют:

- a) процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства в целом
- b) документы и массивы документов, существующие отдельно или в составе информационных систем
- c) государственные тайны и конфиденциальную информацию

36) Разглашение - это...

- a) доведение защищаемой информации до неконтролируемого количества получателей информации
- b) получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней
- c) деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

37) Несанкционированное воздействие на защищаемую информацию - это…

- a) предотвращение ущерба собственнику, владельцу или пользователю информации
- b) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
- c) воздействие с нарушением правил ее изменения

38) Шифрованием информации называют:

- a) процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- b) известность ее содержания только имеющим соответствующие полномочия субъектам
- c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

39) Политика безопасности - это...

- a) состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
- b) это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
- c) это известность ее содержания только имеющим соответствующие полномочия субъектам

40) Контроллер - это...

- a) основное устройство системы, производящее идентификацию пользователя и дающее разрешение на проход, в случае если считанный с идентификатора код совпадает с кодом, хранящимся в памяти контроллера
- b) это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа
- c) это известность ее содержания только имеющим соответствующие полномочия субъектам

41) Основной характеристикой контроллера являются:

- a) комбинированные методы
- b) поддерживаемые режимы работы - автономный или сетевой через линию связи с использованием компьютера
- c) при помощи особых устройств, генерирующих модулированный ультразвуковой, инфракрасный или радиосигнал

42) Идентификация - это...

- a) пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе

- b) информационных ресурсов, систем и технологий является субъект с полномочиями владения и пользования указанными объектами. Под пользователем информации будем понимать субъекта, обращающегося к информационной системе за получением необходимой ему информации и пользующегося ею
- c) пользователь сообщает системе по ее запросу свое имя

43) Основной недостаток подобных систем аутентификации:

- a) информацией в данном случае служит ключ, на котором выполняется шифрование случайного числа. Как видно из схемы обмена, данный ключ никогда не передается по сети, а лишь участвует в вычислениях, что составляет несомненное преимущество протоколов данного семейства
- b) необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование
- c) сервер расшифровывает полученную информацию на том же ключе и сравнивает с исходным случайным числом

44) Самый главный недостаток протокола Kerberos:

- a) необходимость в нескольких специальных серверах
- b) В случае успешной проверки билета сервер TGS генерирует еще один случайный ключ для шифрования сеансов связи между пользователем, желающим получить доступ, и целевым сервером
- c) необходимость иметь на локальном компьютере клиентский модуль, выполняющий шифрование

45) Выбрать правильный ответ, характеризующий протокол идентификации CHAP:

- a) проверяющая система отправляет запрос удаленному устройству, которое запросило подключение к сети
- b) применяет простую процедуру двустороннего обмена для идентификации систем
- c) использует специальный алгоритм для расчета значения, известного только проверяющей системе и удаленному устройству

46) Хешированием информации называют

- a) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации
- b) состояние защищенности информационной среды, обеспечивающее ее формирование и развитие
- c) процесс ее преобразования в хеш -значение фиксированной длины

47) Множество объектов и типов доступа к ним субъекта может изменяться:

- a) в соответствии с некоторыми правилами, существующими в данной системе
- b) статично т.е. не может изменяться вообще
- c) это никак не связано с субъектами

48) Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

- a) все субъекты и объекты системы должны быть идентифицированы
- b) права доступа субъекта к объекту системы определяются без правил
- c) все субъекты и объекты системы должны быть не аутентифицированы

49) Избирательное управление доступом:

- a) концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности
- b) метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
- c) в метод управления доступом субъектов системы к объектам, основанный на опознавании пользователя без любой регистрации

50) Мандатное управление доступом:

- a) метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит
- b) метод доступа субъектов к информационным ресурсам с полной разрешенностью к пользованию информаци
- c) концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности

51) Матрица доступа представляет собой:

- a) прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец
- b) треугольную матрицу, в которой объекту системы соответствует столбец, а субъекту строка
- c) квадратную матрицу, в которой объекту системы соответствует строка, а субъекту столбец

52) Избирательная политика безопасности наиболее широко применяется:

- a) в социальном секторе
- b) в коммерческом секторе
- c) в секторе политики

53) Какие виды резервного копирования поддерживает программа Handy Backup? Выберите несколько вариантов ответа.

a) Полное ✔
b) Выборочное
c) Рабочее
d) Инкрементальное ✔
e) Смешанное ✔
f) Дифференциальное ✔
g) Системное
h) Пользовательское

54) Какие из названных систем резервного копирования являются российскими?

a) Киберпротект ✔
b) Handy Backup ✔
c) Acronis
d) RuBackup ✔
e) Bacula

55) Бесплатная лечащая утилита от российского производителя антивирусов называется:

a) Spider
b) CureIt! ✔
c) Katana
d) vxCube

56) Какой антивирусный продукт Лаборатории Касперского является базовым?

a) Kaspersky Total Security
b) Kaspersky Anti-Virus
c) Kaspersky Internet Security ✔
d) Kaspersky Secure Connection
e) Kaspersky Safe Kids

57) Криптопровайдер это:

a) Компания, реализующая услугу оформления ЭЦП
b) Специальное ПО, реализующее все криптографические алгоритмы ✔

c) Программа, позволяющая формировать пары логин-пароль
d) Удостоверяющий центр, продает токены
58). Простая электронная подпись представляет собой:
a) Аналог собственноручной подписи
b) Выдается аккредитованным удостоверяющим центром
c) Логин и пароль ✔
d) Две уникальные последовательности символов, которые однозначно связаны между собой
59) Санкционированное воздействие на защищаемую информацию - это…
a) предотвращение ущерба собственнику, владельцу или пользователю информации
b) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации
c) воздействие с не нарушением правил ее изменения

60) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность Актуальность
- Доступность. Понятность

3.2. Практические задания (ПЗ)

Раздел 1. ПМ 01. Изучение предмета и задач программно- аппаратных средств

Тема 1.4. Механизмы защиты

Лабораторные работы№1. Способы защиты конфиденциальности, целостности и доступности в КС.

Форма контроля – письменный контроль.

Задание:

Порядок выполнения работы

1. Повторить аппаратные решения для выявления и предотвращения утечек информации.
2. Сделать сравнительный анализ программных компонентов выявления и предотвращения утечек информации.

Оформить отчет по лабораторной работе.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 1. ПМ 01. Изучение предмета и задач программно- аппаратных средств

Лабораторные работы№2. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.

Форма контроля – письменный контроль.

Задание

Для выполнения первой части необходимо для выбранного определенного объекта защиты информации необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

1. виды угроз;
2. характер происхождения угроз;
3. классы каналов несанкционированного получения информации;
4. источники появления угроз;
5. причины нарушения целостности информации;
6. потенциально возможные злоумышленных действий;
7. определить класс защиты информации.

Второе задание

Для выполнения второго задания предложить анализ увеличения защищенности объекта защиты информации по следующим разделам:

1. определить требования к защите информации;
2. классифицировать автоматизированную систему;
3. определить факторы, влияющие на требуемый уровень защиты информации;
4. выбрать или разработать способы и средства защиты информации;
5. построить архитектуру систем защиты информации;
6. сформулировать рекомендации по увеличению уровня защищенности.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 3. Средства и методы ограничения доступа к файлам.

Тема 3.5. Особенности защиты данных от изменения.

Лабораторные работы№1. Изучение криптографических методов защиты при помощи программно-аппаратного комплекса Secret Disk. (Студенты изучают криптографические методы защиты при помощи программно-аппаратного комплекса Secret Disk)

Форма контроля – письменный контроль.

Задание

1. Организация секретного диска.
1. Запустить администратор секретных дисков.
2. Создать секретный диск, который автоматически будет стыковаться при запуске системы. Описать данный диск как «ДИСК1». Выделить объем данному секретному диску – 4Мб, который может расширяться до размера 16 Мб.

3. Задать пароль для доступа к секретному диску. В качестве электронного идентификатора пользователя выбрать электронный ключ HASP. В качестве алгоритма шифрования выбрать алгоритмRC4.

4. Активизировать выданный Вам электронный идентификатор, в результате чего в него запишется случайная последовательность символов. Сгенерированный личный ключ обязательно сохранить на дискете (для возможности отката).

5. Задать пароль для входа в систему под принуждением (который можно сказать злоумышленнику в экстренной ситуации).

6. Сгенерировать рабочий ключ диска и обязательно сохранить его на дискете (для возможности отката).

7. Подключить к системе секретный диск.

8. Открыть в Wordтекстовый документ, внести в него информацию и сохранить на секретном диске.

9. Попытаться в проводнике проводить операции над файлами на секретном диске (копирование – удаление и т.д.).

10. Открыть в Wordсозданный файл с секретного диска.

11. Отключить секретный диск.

12. Попытаться обратиться к открытому файлу в Word. Проследить реакцию системы.

13. Попытаться подключить секретный диск с отключенным идентификатором.

2. Работа с секретным диском.

1. Вызвать параметры созданного секретного диска (диск должен быть отключен). Исследовать информацию, выдаваемую по данному диску. Какую информацию хранит о данном диске система? Какие дополнительные параметры появились в данном окне по сравнению с информацией о стандартных дисках?

2. Какого рода действия предоставляются пользователю в меню «параметры»?

3. Настроить параметры резервного копирования диска. Расположение – на диске С, резервное копирование – перед отключением диска.

4. Реализовать ведение журнала безопасности для данного диска. Тип ведения журнала – циклический.

5. Просмотреть пользователей созданного секретного диска и доступные для администратора операции управления пользователями.

6. Исследовать допустимые настройки в меню «Файл->Параметры системы».

7. Задать для системы тип хранителя экрана – картинка. Задать комбинации клавиш для экстренной блокировки компьютера как “CTRL+SHIFT+1” и красной кнопки ”CTRL+SHIFT+2”.

8. Определить время блокировки компьютера после отключения идентификатора, равное 5 сек.

9. Для «действий при принуждении» задать режим «Синий экран» и «уничтожение содержимого электронного идентификатора».

10. Подключить секретный диск. Отключить идентификатор от компьютера и выждать 5 сек, после чего компьютер будет заблокирован вплоть до подключения идентификатора пользователя.

11. Заблокировать компьютер путем нажатия комбинации клавиш CTRL+SHIFT+1.

12. Отключить секретный диск.

3. Работа в экстренных ситуациях.

1. Подключить секретный диск, после чего воспользоваться комбинацией клавиш «Красная кнопка», что приведет к моментальному отключению секретного диска и уничтожению содержимого электронного идентификатора.

2. Попытаться подключиться к секретному диску после срабатывания «Красной кнопки». Объяснить причину неудачи.

3. Восстановить потерянную информацию первым способом – восстановить с аварийной дискеты личный ключ пользователя и подключиться к секретному диску.

4. Нажать комбинацию клавиш «Красная кнопка».

5. Восстановить потерянную информацию вторым способом 1. Активизировать новый электронный идентификатор 2. Используя аварийную копию рабочего ключа диска, заново задать для диска пароль доступа и личный ключ. Для этого вызвать меню параметров секретного диска, далее изменение пароля и электронного идентификатора, и в качестве файла указать аварийную копию рабочего ключа диска.

6. Заново задать пароль для входа под принуждением.

4. Работа с секретным диском под принуждением.

1. Подключить секретный диск в режиме входа под принуждением. Проследить за реакцией системы.

2. Попытаться подключить секретный диск после перезагрузки системы. Объяснить причину неудачи.

3. Восстановить информацию на диске любым из выше представленных способов.

5. Работа с архивами.

1. Скопировать на секретный диск несколько файлов.

2. Нажать кнопку «сохранить данные». В качестве ключа к архиву указать электронный идентификатор. Алгоритм шифрования – собственный с длиной ключа 128 бит, опцию сжатия.

3. Добавить с секретного диска несколько файлов для архивации и заархивировать их.

4. Попытаться разархивировать данные с электронным идентификатором и без него.

6. Работа с журналом.

1. Вызвать журнал безопасности секретного диска.

2. Исследовать содержание журнала.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 4. Программно-аппаратные средства шифрования

Тема 4.5. Система защиты информации от несанкционированного доступа «Dallas Lock».

Лабораторные работы№1. Изучение методов защиты локальной ПЭВМ от НСД к информации при помощи программно-аппаратного комплекса Dallas Lock 7.0. (Студенты изучают методы защиты от несанкционированного копирования и НСД)

Форма контроля – письменный контроль.

Задание

1. Выполнить очистку остаточной информации

2. Разграничить права доступа администраторов и пользователей к локальным и сетевым ресурсам

3.Разграничить доступ к сменным накопителям для разных пользователей, для пользователя гость закрыть доступ к съемным дискам.

4. Возможность администрирования рабочих мест удаленно.

5.Возможность работы с помощью сервера терминального доступа.

6.Разграничить права по мандатному и дискреционному принципу.

Оформить отче по лабораторной работе.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 5. Методы и средства ограничения доступа к компонентам ЭВМ.

Тема 5.3. Надежность средств защиты компонент.

Лабораторные работы№1. Надежность средств защиты Компонент (Основы работы с персональным межсетевым экраном фирмы «Инфотекс»).

Форма контроля – письменный контроль.

Задание

Провести исследование и системную классификацию средств защиты информации

Приведите и обоснуйте системную классификацию средств защиты информации

Приведите примеры потенциально возможных средств, применяемых для решения задач защиты информации

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 6. Защита программ от несанкционированного копирования.

Тема 6.4. Методы противодействия динамическим способам снятия защиты программ от копирования.

Лабораторные работы№1. Аспекты проблемы защиты от исследования (Основы использования средств защиты от несанкционированного доступа в операционной системе Linux)

Форма контроля – письменный контроль.

Задание

1.Рассмотреть общие вопросы защиты информации

2.Изучить обеспечение информационной безопасности

3.Проанализировать структуру правовой защиты информации

4.Рассмотреть назначение и аспекты правовой защиты информации.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 7. Хранения ключевой информации.

Тема 7.3. Типовые решения в организации ключевых систем.

Лабораторные работы№1. Открытое распределение ключей.

Форма контроля – письменный контроль.

Задание

7. Методические указания к выполнению работы

Лабораторная работа выполняется на ПЭВМ в диалоговом режиме.

После запуска программы Zinf на экране монитора возникает главное меню, на котором нужно выбрать пункт GOST 28147. Возврат в главное меню и выход из него осуществляется кнопкой EXIT. Программа Zinf не контролирует ввод

некорректных данных и ошибочных действий пользователя, поэтому требуется внимательность, а для выхода из тупиковых ситуаций нужно воспользоваться кнопкой EXIT.

Лабораторная программа ГОСТ имитирует процедуры, установленные стандартом для шифрования в режиме

простой замены.

Шифруемый 64-х разрядный блок информации вводится в окна «Блок №1» и «Блок №2» в шестнадцатеричном коде, по 8 шестнадцатеричных цифр в каждое окно. Ввод большего числа цифр программа воспринимает как ошибку.

Ключ, состоящий из 256 разрядов, вводится в 8 окон также в

шестнадцатеричном коде по 8 цифр в каждое окно (Кл. XO, X!, …,X7).

В программе для наблюдения за процессом обработки данных, реализованы 2 варианта работы:

—основной вариант – клавиши «Зашифровать» обеспечивают штатный режим, при котором основной цикл (зашифрование и расшифрование одним из ключей) выполняется непрерывно 32 раза;

—учебный вариант (шаговый режим) – цикл разбит на 5 этапов: суммирование по mod 32, подстановка, сдвиг, суммирование по mod 2, перепись. Нажимая на соответствующие клавиши, можно последовательно наблюдать за поэтапным процессом шифрования.

Для упрощения программы в учебном варианте используется только подключ XO, что соответствует варианту 8 одинаковых подключей.

Другой особенностью программы является вариант реализации подстановок. Стандарт рекомендует для каждой тетрады 32-х разрядного слова S

использовать различные варианты секретных таблиц-подстановок (8 таблиц). В данной учебной программе для ее упрощения реализована одна таблица замен:0→F, 1→E, 2→D, 3→C, 4→B, 5→A, 6→9, 7→8, 8→7, 9→6, A→5, B→4, C→3, D→2, E→1, F→0. В лабораторной программе в целях изучения влияния на качество шифрования подстановок и перестановок (сдвигов), есть возможность отключать любой из этих этапов с помощью флажков. Еще раз обратите внимание на то, что в окна информационных блоков и ключей нельзя вводить больше 8 цифр (меньше – можно) и нельзя делать пробелы в словах.

8. Лабораторное задание

1.Нажатием клавиши ТЕСТ произвести тестовую загрузку информации и ключей.

Освоить работу программы шифрования во всех ее вариантах.

2.Проверить реализацию в данном алгоритме принципа: «Изменение одного символа (бита) в информации должно распространиться на большое число символов криптограммы». Для этого: - ввести тестовую комбинацию; - зашифровать информацию и записать криптограмму в двоичном коде (64 разряда); - изменить один бит в одном из информационных блоков; 7 - провести шифрование в четырех вариантах в зависимости от включения или выключения флажков-этапов подстановки и сдвига. Записать полученные результаты в двоичном коде. 3.Проверить аналогично, реализацию принципа «Изменение одного символа ключа должно распространяться на большое число знаков криптограммы». 4.Проверить работу алгоритма шифрования при «плохих» ключах. Например, ключи из одних нулей (64 шестнадцатеричных «0») или из одних единиц (64 цифры «F»). Записать для каждого случая варианта (по включению флажков) криптограммы в шестнадцатеричном и двоичном кодах.

МДК. 02.01. Программно–аппаратные средства обеспечения информационной безопасности

Раздел 7. Хранения ключевой информации.

Тема 7.3. Типовые решения в организации ключевых систем

Лабораторные работы№2. Метод управляемых векторов.

Форма контроля – письменный контроль.

Задание

Используя правила работы с векторами построить графики заданных функций одной переменной на отрезках, наиболее характерных для отображения сущности функций. Графики вывести различными способами: в отдельные графические окна,в одно окно на одни оси,в одно окно на отдельные оси.

Определить экстремумы функции.

Вывести результаты в табличном виде.

Сохранить результаты в файле.

Выполнить контрольные просчеты.

Выполнить одно из следующих заданий по работе с векторами. Способ решения задач должен носить универсальный характер и быть пригодным для произвольных векторов (в качестве данных для контроля решения задачи следует использовать результаты работы с заданными функциями):

Выделить в новые векторы элементы вектора с большими и меньшими значениями.

Выделить в новые векторы элементы вектора с четными и нечетными номерами.

Найти суммы положительных и отрицательных элементов вектора.

Заменить элементы вектора, отличающиеся от среднего геометрического его элементов более чем на 10%, на среднее геометрическое.

Заменить все минимальные элементы вектора максимальным значением его элементов.

Определить количество положительных, отрицательных и нулевых элементов вектора.

Найти число элементов вектора, отличающихся от среднего арифметического меньше, чем на 20%.

Заменить элементы вектора, отличающиеся от нулевого уровня не более чем на 5%, на ноль.

Заменить элементы вектора, отличающиеся от максимального положительного значения не более чем на 5%, на максимальное.

Заменить элементы вектора, отличающиеся от минимального отрицательного значения не более чем на 5%, на минимальное.

Определить номер элемента вектора с наибольшим отклонением от среднего арифметического всех элементов вектора.

Вычислить суммы всех элементов вектора с четными и нечетными индексами.

Вычислить произведение элементов вектора, не превосходящих среднее арифметическое значение его элементов.

Определить количество положительных элементов вектора, расположенных между его максимальным и минимальным элементами.

Заменить положительные элементы вектора суммой всех его отрицательных элементов.

3.2. Контрольные вопросы (КВ)

КВ № 1. Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации

КВ № 2. Классификация методов и средств программно-аппаратной защиты информации.

КВ № 3. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)

КВ № 4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

КВ № 5. Автоматизация процесса обработки информации. Понятие автоматизированной системы. Методы создания безопасных систем

КВ № 6. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.

КВ № 7. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели

КВ № 8. Источники дестабилизирующего воздействия на объекты защиты. Причины и условия дестабилизирующего воздействия на информацию

КВ № 9. Способы воздействия на информацию. Понятие несанкционированного доступа к информации

КВ № 10. Основные подходы к защите информации от НСД

КВ № 11. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса

КВ № 12. Особенности защиты данных от изменения. Шифрование.
КВ № 13. Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды.
КВ № 14. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.
КВ № 15. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение
КВ № 6. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.
КВ № 17. Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
КВ № 18. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.
КВ № 19. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме"
КВ № 20. Основные концепции построения систем антивирусной защиты на предприятии. Несанкционированное копирование программ как тип НСД
КВ № 21. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
КВ № 22. Привязка ПО к аппаратному окружению и носителям. Проблема защиты отчуждаемых компонентов ПЭВМ.
КВ № 23. Защитные механизмы в современном программном обеспечении на примере MS Office.
КВ № 24. Методы защиты информации на отчуждаемых носителях. Шифрование.
КВ № 25. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
КВ № 26. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов
КВ № 27. Безвозвратное удаление данных. Принципы и алгоритмы.
КВ № 28. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
КВ № 29. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ
КВ № 30. Использование сетевых снифферов в качестве СОВ
КВ № 31. Аппаратный компонент СОВ. Программный компонент СОВ.
КВ № 32. Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.
КВ № 33. Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP.

КВ № 34. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.
КВ № 35. Виртуальная частная сеть. Функции, назначение, принцип построения
КВ № 36. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
КВ № 37. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Методы защиты информации при работе в сетях общего доступа.
КВ № 38. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall.
КВ № 39. Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня.
КВ № 40. Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.
КВ № 41. Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом Средства контроля целостности информации в базах данных
КВ № 42. Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных
КВ № 43. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации
КВ № 44. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25
КВ № 45. Классификация отслеживаемых событий. Особенности построения систем мониторинга
КВ № 46. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов
КВ № 47. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.
КВ № 48. Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.

4. 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.

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. 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.

6. Криптографическая защита информации в объектах информационной инфраструктуры:учебник, 1-е изд.,/ Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - ИЦ Академия, 2020 -288 с

7. 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

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:

IPRBOOKS - 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/

1.