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

Комплект контрольно-оценочных средств

междисциплинарного курса

МДК 02.01 Программные и программно-аппаратные средства защиты информации

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2022

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

Составитель:
Ляшенко А.В., 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 междисциплинарного курса МДК 02.01Программные и программно-аппаратные средства защиты информации. КОС включают контрольные материалы для проведения текущей и промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы междисциплинарного курса.

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:

3.1	особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
3.2	методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
3.3	типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
3.4	основные понятия криптографии и типовых криптографических методов и средств защиты информации;
3.5	особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
3.6	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 «Администратор баз данных», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 22 января 2013 г. N 23, который актуализируются при изучении междисциплинарного курса:

1) Обеспечение функционирования БД;
2) Предотвращение потерь и повреждений данных;
3) Обеспечение информационной безопасности на уровне БД;
4) Управление развитием БД.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Ворлдскиллс Сетевое и системное администрирование, которые актуализируются при изучении междисциплинарного курса:

1) знать и понимать: как настраивать коммутацию уровня доступа, агрегации и ядра;

2) знать и понимать: как настраивать протоколы маршрутизации внутреннего и внешнего шлюза;

3) знать и понимать: как обеспечивать отказоустойчивость сети на уровне коммутации и маршрутизации;

4) знать и понимать: как применять базовые механизмы защиты от компрометации активного сетевого оборудования;

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 - Соадминистрирование баз данных и серверов, в том числе общими компетенции (ОК) и профессиональными компетенциями (ПК):

Код	**Наименование результата обучения**
ОК 1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9	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 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 1	КВ 1
Тема 1.2. Стандарты безопасности	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 2	КВ 2

Тема 1.3. Защищенная автоматизированная система	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 3	КВ 3
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 4	КВ 4
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 5	КВ 5
Тема 2.1. Основы защиты автономных автоматизированных систем	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 6	КВ 6
Тема 2.2.Защита программ от изучения	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 7	КВ 7
Тема 2.3. Вредоносное программное обеспечение	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 8	КВ 8
Тема 2.4. Защита программ и данных от несанкционированного копирования	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 9	КВ 9
Тема 2.5. Защита информации на машинных носителях	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	пЗ 10	КВ 10
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 11	КВ 11
Тема 2.7. Системы обнаружения атак и вторжений	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 12	КВ 12
Тема 3.1.	ОК1 – 2,9,8	ПЗ 13	КВ 13

Основы построения защищенных сетей	ПК 7.1 У3 З1 ЛР 1		
Тема 3.2. Средства организации VPN	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 14	КВ 14
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 15	КВ 15
Тема 5.1. Защита информации в базах данных	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 16	КВ 16
Тема 6.1. Мониторинг систем защиты	ОК3-4,10 ПК 7.2 У2 З2 ЛР 1	ПЗ 17	КВ 17
Тема 6.2. Изучение мер защиты информации в информационных системах	ОК5-6, 11 ПК 7.3 У1 З1 ЛР 1	ПЗ 18	КВ 18
Тема 6.3. Изучение современных программно-аппаратных комплексов.	ОК1 – 2,9,8 ПК 7.1 У3 З1 ЛР 1	ПЗ 19	КВ 19
экзамен	ОК 1-11, ПК 7.1-7.3 У 1-3 З 1-2		ТЗ № 1-20

2. Комплект оценочных средств для текущей аттестации

2.1. Практические задания (ПЗ)

ПЗ №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

ПЗ №2 Руководящие документы. Гостехкомиссии по оценке защищенности от НСД.

Форма контроля –письменный контроль.

ЗаданиеДля 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.

ПЗ № 3 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. Задание1.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 журнал

ПЗ № 4 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.

ПЗ №5 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

ПЗ № 6 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.

ПЗ № 7 Открытое распределение ключей.

Форма контроля –письменный контроль.

Задание7. 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.

ПЗ № 8 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

ПЗ № 9 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.

Цель: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1.Предмет и задачи программно-аппаратной защиты информации

.2.Основные понятия программно-аппаратной защиты информации.

3.Классификация методов и средств программно-аппаратной защиты информации.

4.Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.

ПЗ 10 Обзор стандартов. Работа с содержанием стандартов

Цели: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1.Предмет и задачи программно-аппаратной защиты информации.

2.Основные понятия программно-аппаратной защиты информации.

3.Классификация методов и средств программно-аппаратной защиты информации.

4.Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 1. Выписать государственные стандарты в области информационной безопасности. Задание

2. Выписать международные стандарты информационной безопасности. Задание

3. Изучить ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология.

Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами

ПЗ 11 Учет, обработка, хранение и передача информации в АИС

Цели: познакомиться со способами учета, обработки, хранения и

передачи информации в АИС.

Теоретические вопросы

1.Технологии учета и хранения информации.

2.Технологический процесс обработки информации.

3.Способы обработки информации.

4.Режимы обработки информации на компьютере.

5.Технологии передачи и представления информации.

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации.

В чем заключается различие между централизованным и децентрализованным способами обработки информации?

Какие режимы обработки информации вам известны?

ПЗ 12 Ограничение доступа на вход в систему

Цель: ознакомиться с процедурами создания учётных записей пользователей и управления их правами.

Теоретические вопросы

1.Учётные записи пользователей.

2.Создание учётных записей пользователей.

3.Создание учётных записей пользователей для компьютеров, состоящих в рабочей группе.

4.Создание учётной записи при помощи оснастки «Локальные пользователи и группы».

5.Создание учётной записи при помощи командной строки.

6.Управление учётными записями при помощи диалога «Управление учётными записями пользователей».

Задание 1. Ознакомиться с технологиями создания и управления учетными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

Задание 2. Создайте новую учетную запись пользователя с помощью командной строки. Задание Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

Задание 4. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя

ПЗ № 13 Идентификация и аутентификация пользователей

Цель: ознакомиться с механизмами идентификации и аутентификации пользователей.

Теоретические вопросы

1.Понятия идентификации и аутентификации пользователей.

2.Механизмы аутентификации и идентификации пользователей.

Задание 1. Опишите параметры локальной политики безопасности операционной системы Windows:

–кто имеет доступ к компьютеру;

–какие ресурсы могут использовать пользователи на компьютере;

–включение и выключение записи действий пользователей или группы пользователей в журнале событий.

ПЗ 14 Разграничение доступа.

Цель: освоение навыков управления доступом пользователей.

Теоретические вопросы

1.Стандартные разрешения для файлов и папок.

2.Механизмы разграничения доступа.

3.Списки управления доступом ACL.

4.Реализация дискреционной модели доступа в ОС Windows.

Задание 1. Выполните задания.

•Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

•Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

•Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

•Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

•Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

•Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

•Составьте отчет о проведенных экспериментах.

Задание 2. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей

ПЗ 15 Регистрация событий (аудит)

Цель: ознакомиться с механизмами регистрации событий.

Теоретические вопросы

1.Понятия регистрации и аудита.

2.Средства регистрации и аудита.

3.События, фиксируемые в системном журнале.
Задание 1
ОпишитепараметрыизначенияпараметровПолитикиаудита.Заполнитьтаблицу.
Задание 2. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале?
Задание 3. Включите аудит успеха и отказа всех параметров.
Задание 4. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись.
Задание 5. Удалите раннее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием

ПЗ №16 Контроль целостности данных
Цели: получить навыки обнаружения фактов изменения данных, контроля целостности данных с помощью механизма хэш-функций.
Теоретические вопросы
1.Хэш-функция.
2.Свойствахэш-функции.
3.Области использования хэш-функции.
4.Вычислениехэш-функции.

ПЗ № 17 Уничтожение остаточной информации
Цель: ознакомиться с механизмами уничтожения остаточной информации.
Теоретические вопросы
1.Определение остаточной информации.
2.Причины возникновения остаточной информации.
3.Уничтожение информации как часть процесса обеспечения информационной безопасности.
4.Анализ современных методов и средств ликвидации информации с магнитных носителей.
Задание 1. Опишите причины возникновения остаточной информации.
Задание 2. Приведите примеры устройств уничтожения информации с магнитных носителей.
Задание 3. Изучите особенности современных методов ликвидации информации на магнитных носителях

ПЗ № 18 Управление политикой безопасности. Шаблоны безопасности
Цель: ознакомиться с механизмами управления политикой безопасности.
Теоретические вопросы
1.Дискреционная политика безопасности.
2.Доменыбезопасности.
3.Матрицадоступа.
4.Мандатная политика безопасности.

ПЗ № 19 Криптографическая защита.
Обзор программ шифрования данных
Цель: ознакомиться с программами шифрования данных.
Теоретические вопросы
1.Понятия криптографии и крипто анализа.
2.Симметричные и асимметричные криптографические системы.
3.Криптостойкостьшифра.
4.Алгоритмышифрования.
5.Программы шифрования данных
6.Требования к крипто системам.
Задание 1. Разработать алгоритм шифрования данных.
Задание 2. Привести примеры программ шифрования данных.
Задание 3. Провести сравнительный анализ программ шифрования данных.
Задание 4. Описать возможности одной из программ шифрования данных.

3. Комплект оценочных средств для промежуточной аттестации

3.1. Практические задания (ПЗ)

3.2. Тестовые задания (ТЗ)

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

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

	Б) Протокол Kerberos В) Аутентификация по биометрическим характеристикам Г) Аутентификация по росписи мышью
11. Целью защиты информации является:	А) предотвращение хищения, утечки, искажения, утраты и подделки информации; **Б) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;** В) реализация права на государственную тайну и конфиденциальную информацию Г) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации
12. К основным видам средств защиты информации относится:	**А) нормативно-правовые** **Б) Технические** В) Экологические Г) Этнические
13. Технические средства защиты – это	А) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации **Б) это комплексы специального технического и программного обеспечения** В) правила и нормы поведения, направленные на обеспечение безопасности информации Г) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе
14. К каналам утечки информации относится:	**А) Магнитный канал** **Б) Виброакустический канал** **В) Лазерный канал** Г) Специальный канал
15. К назначению ОС относится:	А)управление процессором путем чередования выполнения программ; Б)обработка прерываний и синхронизация доступа к ресурсам вычислительной

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

3.3. Контрольные вопросы (КВ)

КВ 1. Концепция информационной безопасности.
КВ 2. Каналы утечки информации.
КВ 3. Виды ПО. Назначение и функции ОС.
КВ 4. Классификация операционных систем.

КВ 5. Локальные и удаленные атаки и методы взлома ОС.
КВ 6. Защита от локального НСД.
КВ 7. Протокол Kerberos.
КВ 8. Протокол S/key
КВ 9. Идентификация и аутентификация.
КВ 10.Подсистема аутентификации Windows.
КВ 11. Разграничение доступа.
КВ 12. Избирательный и мандатный метод разграничения доступа.
КВ 13. Аудит.
КВ 14. Политика аудита.
КВ 15. Фрагментарный и комплексный подход к построению ОС.
КВ 16. Методы анализа сетевой информации.
КВ 17. Защищенность БД
КВ 18. Модели безопасности БД

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.

Электронные издания (электронные ресурсы):

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с. https://urait.ru/bcode/451933

Цифровая образовательная среда СПО PROFобразование:

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

Электронно-библиотечная система:

IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:
Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/