КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Оценочные материалы по дисциплине Защита в операционных системах

обсуждены и рекомендованы к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрены Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

Целью оценочные материалы по дисциплине (модулю) (далее –ОМ) является комплексная оценка результатов обучения по дисциплине Защита в операционных системах и установление уровня сформированности компетенций обучающегося.

ОМ предназначен для проведения текущего контроля успеваемости и промежуточной аттестации.

ОМ включает оценочные средства для проведения текущего контроля успеваемости и промежуточной аттестации.

Оценочные материалы разработаны в соответствии с рабочей программой дисциплины Защита в операционных системах.

1. Паспорт оценочных материалов по дисциплине «Защита в операционных системах»

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения.	ОПК-12.1 Применяет знания основных принципов функционирования операционных систем при выполнении работ по восстановлению работоспособности прикладного и системного программного обеспечения	Знать: основные основных принципов функционирования операционных систем при выполнении работ по восстановлению работоспособности прикладного и системного программного обеспечения. Уметь: функционировать операционными системами. Владеть: навыками применения, при выполнении работ по восстановлению работоспособности прикладного и системного программного обеспечения	Тема 1. Архитектура безопасности современных операционных систем	Реферат (Тема 1) Тест (тема 1)	Тест (П 1-6 тестового задания)
	ОПК-12.2 Имеет практический опыт администрирования операционных систем общего и специального назначения в части их функционирования,	Знать: практическийопыт администрирования операционных систем общего и специального назначения в части их функционирования, инсталляции и технического сопровождения Уметь: проводить детальное исследование операционных систем общего и специального назначения в части их функционирования,	Тема 1. Основные понятия баз данных. Тема 2. Системы управления базами данных.	Реферат (Тема 2-4) Тест (Тема 2) Практическое задание (Тема 1-2)	Тест (П 7-21 тестового задания)

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения	Контролируемые разделы, темы дисциплины	Наименование оценочного средства	
				Текущий контроль	Промежуточная аттестация
1	2	3	4	5	6
	инсталляции и технического сопровождения; а также программных средств специального назначения, входящих в состав этих операционных систем	инсталляции и технического сопровождения; Владеть: навыками практической работы функционирования, инсталляции и технического сопровождения.			

2. Оценочные материалы по дисциплине «Защита в операционных системах»

2.1 Оценочные материалы для проведения текущего контроля успеваемости

Тематика рефератов

Тема 1. Архитектура безопасности современных операционных систем

Содержание: модели безопасности (DAC, MAC, RBAC), ядро и его роль в обеспечении безопасности, уровни привилегий (ring 0–3), подсистема безопасности Windows (LSASS, SRM), SELinux и AppArmor в Linux.

Доклады:

1. Сравнение моделей управления доступом: DAC, MAC, RBAC.
2. Архитектура безопасности Windows: от Windows NT до Windows 11.
3. SELinux: принципы работы и применение в корпоративных средах.
4. AppArmor vs SELinux: сравнительный анализ.
5. Роль микроядра и гипервизора в повышении безопасности ОС.

Тест:

1. Какая модель управления доступом реализована в большинстве дистрибутивов Linux по умолчанию?
   a) MAC
   b) DAC
   c) RBAC
   d) ABAC
2. Какой компонент Windows отвечает за проверку прав доступа?
   a) Winlogon
   b) LSASS
   c) Security Reference Monitor
   d) SAM
3. Что означает аббревиатура SELinux?
   a) Secure Enhanced Linux
   b) Systematic Enforcement Linux
   c) Security-Enhanced Linux
   d) Standard Enterprise Linux
4. Какой уровень привилегий имеет ядро ОС на x86-архитектуре?
   a) Ring 1
   b) Ring 2
   c) Ring 3
   d) Ring 0

5. Какая модель управления доступом используется в военных системах?

a) DAC
b) RBAC
c) MAC
d) ACL

Тема 2. Управление пользователями и правами доступа

Содержание: локальные и доменные учётные записи, группы, политики паролей, UAC, sudo и привилегии в Linux, ACL и расширенные права в Windows и POSIX.

1. Принцип наименьших привилегий в администрировании ОС.
2. Настройка и аудит групп безопасности в Active Directory.
3. Роль sudo в защите Linux-систем.
4. Политики паролей и их влияние на безопасность.
5. Различия между ACL в Windows и POSIX.

Тест:

1. Какая утилита в Linux позволяет временно выполнять команды от имени root?
    a) login
    b) su
    c) sudo
    d) passwd
2. Какой механизм в Windows предотвращает несанкционированное повышение привилегий?
    a) BitLocker
    b) UAC
    c) Firewall
    d) Defender
3. Что такое SID в Windows?
    a) Сертификат безопасности
    b) Идентификатор безопасности
    c) Ключ шифрования
    d) Имя пользователя
4. Какой файл в Linux содержит список пользователей?
    a) /etc/passwd
    b) /etc/shadow
    c) /etc/group
    d) /etc/sudoers
5. Какой тип группы в AD используется для предоставления доступа к ресурсам?
    a) Глобальная
    b) Универсальная
    c) Локальная домена
    d) Встроенные

Тема 3. Аудит и мониторинг безопасности ОС

Содержание: журналы событий (Windows Event Log, syslog, journald), централизованный сбор логов, SIEM, настройка аудита объектов доступа, инструменты: auditd, Wazuh, OSSEC.

1. Журналы безопасности в Windows: типы событий и их анализ.
2. Настройка auditd для отслеживания критических операций в Linux.
3. Централизованный сбор логов: архитектура и инструменты.
4. Обнаружение подозрительной активности через анализ логов.
5. SIEM-системы: интеграция с ОС для обнаружения атак.

Тест:

1. Какой сервис в Linux отвечает за сбор системных логов по умолчанию в современных дистрибутивах?
    a) syslog
    b) rsyslog
    c) systemd-journald
    d) auditd
2. Какой журнал Windows содержит события входа/выхода пользователей?
    a) System
    b) Application
    c) Security
    d) Setup
3. Какая утилита в Linux позволяет настраивать аудит файловых операций?
    a) logwatch
    b) auditd
    c) fail2ban
    d) journalctl
4. Что такое SIEM?
    a) Система шифрования дисков
    b) Система управления инцидентами и мониторинга событий
    c) Протокол аутентификации
    d) Фаервол
5. Какой уровень важности события обозначается как "error" в syslog?
    a) 0
    b) 3
    c) 5
    d) 7

Тема 4. Защита от вредоносного ПО и эксплойтов

Содержание: механизмы защиты памяти (DEP, ASLR, SMEP), антивирусы, EDR, sandboxing, AppLocker, защита от буферных переполнений, zero-day угрозы.

1. Механизмы защиты памяти в современных ОС: DEP, ASLR, CFI.
2. Как работает эксплойт и как ему противостоять.
3. Роль EDR-систем в защите корпоративных ОС.
4. AppLocker и Software Restriction Policies: блокировка недоверенного ПО.
5. Песочницы и изоляция приложений в Windows и Linux.

Тест:

1. Какой механизм предотвращает выполнение кода из стека?
    a) ASLR
    b) DEP
    c) SMEP
    d) UAC
2. Что делает ASLR?
    a) Шифрует память
    b) Случайным образом размещает модули в памяти
    c) Блокирует запуск .exe-файлов
    d) Удаляет временные файлы
3. Какая технология относится к EDR?
    a) Windows Defender Antivirus
    b) Microsoft Defender for Endpoint
    c) BitLocker
    d) Windows Hello
4. Какой из перечисленных — НЕ метод защиты от эксплойтов?
    a) DEP
    b) ASLR
    c) AppArmor
    d) NAT
5. Какой компонент Windows позволяет ограничить запуск ПО по хэшу или пути?
    a) UAC
    b) AppLocker
    c) LSASS
    d) SAM

Критерии оценки выполнения рефератов по учебной дисциплине

Оценка «отлично» выставляется студенту, если тема реферата раскрыта в полной мере и все требования по написанию реферата соблюдены.

Оценка «хорошо» выставляется студенту, если недостаточно раскрыта тема реферата, но все требования по написанию реферата соблюдены.

Оценка «удовлетворительно» выставляется студенту, если недостаточно раскрыта тема реферата, не все требования по написанию реферата соблюдены, присутствуют ошибки и неточности в работе.

Оценка «неудовлетворительно» выставляется студенту, если отсутствует реферат.

Рекомендации по написанию реферата:

Реферат — письменная работа, выполняемая обучающимся в течение определенного срока.

Реферат — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях). Реферат — не механический пересказ работы, а изложение ее существа.

Кроме реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата предлагает преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.

2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.

4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.

5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.

6. Приложение может включать графики, таблицы, расчеты.

7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;

2. Изложение результатов изучения в виде связного текста;

3. Устное сообщение по теме реферата.

1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями.

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов,

фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и фиксируют устойчивые и несомненные суждения. В текстах-рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, - т. е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать, и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение.

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемые к оформлению реферата

Объемы рефератов – от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,

– дословное переписывание книг, статей, заимствования рефератов из интернета и т. д.

При проверке реферата преподавателем оцениваются:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).

5. Использование литературных источников.

6. Культура письменного изложения материала.

7. Культура оформления материалов работы.

Комплект типовых практических заданий

Тема 1. Архитектура и модели безопасности операционных систем

Содержание темы: одели управления доступом: дискреционная (DAC), мандатная (MAC), ролевая (RBAC). Архитектура подсистемы безопасности в Windows (LSASS, SAM, Security Reference Monitor). Реализация безопасности в Linux: SELinux, AppArmor. Уровни привилегий процессора (ring 0–3). Принципы изоляции, целостности и конфиденциальности в ОС.

Вопросы для самоконтроля:

1. Какие модели управления доступом применяются в современных ОС?
2. В чём различие между DAC и MAC?
3. Какие компоненты составляют подсистему безопасности Windows?
4. Что такое Security Reference Monitor и какова его роль?
5. Как SELinux реализует мандатный контроль доступа?

Цель работы – получение теоретических знаний и практических навыков анализа архитектуры безопасности операционных систем.
В работе используется презентация, выполненная в MS PowerPoint.

Тема 2. Управление пользователями и правами доступа

Содержание темы: учётные записи, группы, политики паролей. Принцип наименьших привилегий. UAC в Windows, sudo в Linux. ACL (Access Control Lists) в POSIX и Windows NT. Аудит прав доступа к файлам и каталогам.

Вопросы для самоконтроля:

1. Какие типы учётных записей существуют в ОС?
2. Что такое принцип наименьших привилегий?
3. Как работает механизм UAC в Windows?
4. Как в Linux настроить запуск команд от имени root без полного входа?
5. Чем отличаются ACL в Windows и в Linux?

Цель работы – формирование навыков безопасного управления пользователями и разграничения доступа в ОС.

В работе используется презентация, выполненная в MS PowerPoint.

Тема 3. Аудит и мониторинг безопасности

Содержание темы: ;урналы событий: Windows Event Log, syslog, journald. Настройка аудита объектов доступа. Инструменты: auditd (Linux), Advanced Audit Policy (Windows). Централизованный сбор логов. Введение в SIEM-системы.

Вопросы для самоконтроля:

1. Какие типы журналов событий ведутся в Windows?
2. Как включить аудит входа пользователей в Linux?
3. Что позволяет отслеживать служба auditd?
4. Какие события следует аудировать в целях безопасности?
5. Что такое SIEM и как он связан с логами ОС?

Цель работы – развитие навыков настройки и анализа систем аудита для выявления подозрительной активности.
В работе используется презентация, выполненная в MS PowerPoint.

Тема 4. Защита от вредоносного ПО и эксплойтов

Содержание темы: механизмы защиты памяти: DEP, ASLR, SMEP, CFG. Антивирусы и EDR-решения. AppLocker, Software Restriction Policies. Песочницы и изоляция приложений. Анализ уязвимостей и zero-day угроз.

Вопросы для самоконтроля:

1. Как DEP предотвращает выполнение вредоносного кода?
2. Что такое ASLR и как он усложняет эксплуатацию уязвимостей?
3. Какие технологии относятся к классу EDR?
4. Как AppLocker ограничивает запуск недоверенных программ?
5. В чём преимущество изоляции приложений в песочнице?

Цель работы – освоение механизмов защиты ОС от современных угроз на уровне ядра и приложений.

В работе используется презентация, выполненная в MS PowerPoint.

Тема 5. Шифрование данных в операционных системах

Содержание темы: шифрование дисков: BitLocker (Windows), LUKS (Linux). Шифрование файлов: EFS. Роль TPM. Ключи восстановления и безопасное управление ими. Шифрование съёмных носителей.

Вопросы для самоконтроля:

1. Какие технологии шифрования дисков используются в Windows и Linux?
2. Что такое TPM и как он используется в BitLocker?
3. В чём разница между BitLocker и EFS?
4. Как обеспечивается восстановление зашифрованных данных при утере пароля?
5. Почему шифрование съёмных носителей критически важно для безопасности?

Цель работы – освоение методов защиты конфиденциальных данных на уровне файловой системы и физического носителя.

В работе используется презентация, выполненная в MS PowerPoint.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Тема 1. Управление пользователями и правами доступа в ОС

Цель работы – формирование практических навыков безопасного управления учётными записями и разграничения доступа к ресурсам в операционных системах.

В работе используется виртуальная машина с установленной операционной системой (Windows 10/11 или Ubuntu Linux).

1. Настроить в Windows две учётные записи пользователей (например, user1, user2) и одну группу developers. Назначить обе учётные записи в группу. Создать папку C:\Projects, установить права доступа так, чтобы только члены группы developers могли читать и изменять содержимое папки. Проверить доступ от имени каждого пользователя.
2. Настроить в Linux двух пользователей (dev1, dev2) и группу webdev. Создать каталог /var/www/shared, назначить группу-владельца webdev, установить права 775. Добавить обоих пользователей в группу. Проверить, что оба могут создавать и редактировать файлы в каталоге.
3. Изменить политику паролей в Windows (через «Локальная политика безопасности»): минимальная длина — 10 символов, обязательное использование сложного пароля. Применить и проверить на новом пользователе.
4. Настроить в Linux запуск команды systemctl status nginx через sudo без ввода пароля для пользователя webuser. Протестировать команду.
5. Создать скрипт на Bash, который выводит список всех пользователей, входивших в систему за последние 24 часа (используя last или journalctl). Запустить скрипт и проанализировать вывод.

Тема 2. Аудит и мониторинг безопасности

Цель работы – формирование практических навыков настройки и анализа журналов безопасности в операционных системах.

В работе используется виртуальная машина с ОС Windows и/или Linux.

1. Включить расширенный аудит в Windows (через «Политика безопасности → Аудит»): аудит входа/выхода, доступа к объектам, изменения политик. Выполнить попытку входа и просмотреть журнал событий (Event Viewer) — найти соответствующие записи в разделе «Безопасность».
2. Установить и настроить службу auditd в Linux. Создать правило аудита для отслеживания доступа к файлу /etc/passwd. Попытаться прочитать файл от имени обычного пользователя и проверить лог /var/log/audit/audit.log.
3. С помощью PowerShell (Windows) или journalctl (Linux) найти все события за последние 2 часа, связанные с запуском или остановкой служб.
4. Создать простой скрипт на Bash, который раз в 5 минут проверяет, запущен ли критический процесс (например, sshd), и при его отсутствии отправляет уведомление в системный журнал (logger).
5. Проанализировать журнал безопасности Windows и выявить (условно) подозрительную активность: несколько неудачных попыток входа подряд. Оформить краткий отчёт (2–3 предложения) с указанием времени, имени пользователя и источника.

Тема 3. Защита данных и шифрование в ОС

Цель работы – формирование практических навыков шифрования данных на уровне файловой системы в операционных системах.

В работе используется виртуальная машина с Windows и/или Linux.

1. В Windows с помощью BitLocker зашифровать внешний USB-накопитель (или виртуальный диск). Сохранить ключ восстановления в файл. Выполнить чтение/запись данных после разблокировки.
2. В Linux создать зашифрованный раздел с помощью LUKS (используя cryptsetup). Смонтировать его в каталог /mnt/secret, создать файл внутри, размонтировать и снова смонтировать — убедиться, что данные сохранены.
3. Зашифровать отдельный файл в Windows с помощью EFS (ПКМ → Свойства → Дополнительно → «Шифровать…»). Проверить, что файл недоступен другому пользователю.
4. Создать резервную копию ключа BitLocker и сохранить её в безопасном месте (например, на другом виртуальном диске). Продемонстрировать восстановление доступа.
5. Сравнить производительность чтения/записи на зашифрованном и незашифрованном разделах (условно, на основе наблюдений). Сделать вывод о влиянии шифрования на производительность.

Тема 4. Безопасная конфигурация и харденинг ОС

Цель работы – формирование практических навыков снижения поверхности атаки за счёт безопасной настройки операционной системы.

В работе используется виртуальная машина с Linux (Ubuntu) или Windows.

1. Отключить ненужные службы и демоны в Linux: cups (печать), avahi-daemon (обнаружение в сети).
2. Проверить с помощью systemctl list-units --type=service --state=running.
3. Настроить правила ufw (Uncomplicated Firewall) в Linux: разрешить только SSH (порт 22) и HTTP (порт 80); запретить всё остальное.
4. Проверить доступность портов с другого хоста (например, через nmap).
5. В Windows отключить ненужные функции: SMBv1, удалённый реестр, автоматическое воспроизведение.
6. Использовать «Включение или отключение компонентов Windows» и редактор реестра.
7. Применить базовые рекомендации CIS к Linux: установить пароль на загрузчик GRUB, отключить вход по умолчанию для root, настроить автоматические обновления.
8. Создать скрипт на PowerShell (Windows) или Bash (Linux), который проверяет наличие обновлений безопасности и выводит статус («Обновления доступны» / «Система актуальна»).

Критерии оценки:

Оценка «отлично» - студент показывает полные и глубокие знания программного материала, логично и правильно выполняет практическое задание, показывает высокий уровень теоретических знаний.

Оценка «хорошо» - студент показывает хорошие знания программного материала, задание выполнено, но содержит небольшие несущественные погрешности.

Оценка «удовлетворительно» - студент показывает достаточные, не полные знания программного материала, задание выполнено с большим количеством ошибок.

Оценка «неудовлетворительно» - студент показывает недостаточные знания программного материала, задание выполнено неправильно или отсутствует полностью.

2.2 Оценочные материалы для проведения промежуточной аттестации

Вопросы к зачёту:

1. Понятие защиты в операционных системах. Основные цели и задачи.

2. Модели управления доступом: DAC, MAC, RBAC — определение и сравнение.
3. Архитектура подсистемы безопасности в Windows (LSASS, SAM, SRM).
4. Что такое Security Reference Monitor и какова его роль?
5. Принцип наименьших привилегий — формулировка и применение.
6. Уровни привилегий процессора (ring 0–3) и их значение для безопасности.
7. Что такое SID в Windows и как он используется?
8. Управление пользователями и группами в Windows: основные инструменты.
9. Управление пользователями в Linux: файлы /etc/passwd, /etc/shadow, /etc/group.
10. Роль sudo в обеспечении безопасности Linux-систем.
11. Настройка групповых политик безопасности в Windows.
12. Что такое ACL и как они применяются в Windows и Linux?
13. Отличия POSIX ACL от расширенных ACL в Windows.
14. Журналы событий Windows: типы, структура, ключевые категории (Security, System, Application).
15. Как включить аудит входа пользователей в Windows?
16. Служба auditd в Linux: назначение и основные возможности.
17. Как настроить аудит доступа к критическому файлу в Linux?
18. Что такое SIEM и как он интегрируется с ОС?
19. Механизмы защиты памяти: DEP, ASLR, SMEP, CFG — назначение каждого.
20. Как DEP предотвращает выполнение вредоносного кода?
21. Принцип работы ASLR и его влияние на эксплуатацию уязвимостей.
22. Что такое EDR и какие функции он выполняет?
23. AppLocker: назначение, возможности, сценарии использования.
24. Программные песочницы: примеры и принципы изоляции.
25. Основные угрозы, связанные с вредоносным ПО в ОС.
26. Шифрование дисков в Windows: BitLocker — требования и архитектура.
27. Роль TPM в защите ключей BitLocker.
28. Шифрование отдельных файлов в Windows: EFS — принцип работы и ограничения.
29. Шифрование дисков в Linux: LUKS — структура и настройка.
30. Безопасное управление ключами восстановления при шифровании.
31. Шифрование съёмных носителей: риски и методы защиты.
32. CIS Benchmarks — что это и как применяются?
33. Харденинг ОС: основные этапы и рекомендации.

34. Какие службы рекомендуется отключать при харденинге?
35. Настройка встроенного фаервола в Windows и Linux.
36. Применение автоматизированных инструментов (Ansible, Puppet) для харденинга.
37. Обновления безопасности: важность и методы управления.
38. Безопасность виртуальных машин: угрозы и меры защиты.
39. Что такое VM escape и как ему противостоять?
40. Безопасность гипервизоров (Type 1 и Type 2).
41. Особенности безопасности VMware, Hyper-V, KVM.
42. Контейнеризация и безопасность: в чём отличие от виртуализации?
43. Изоляция в Docker: namespaces, cgroups, capabilities.
44. Что такое seccomp и как он повышает безопасность контейнеров?
45. Подпись образов контейнеров (image signing) — зачем и как.
46. Уязвимости в образах Docker и методы их сканирования.
47. SELinux: архитектура, политики, режимы работы (enforcing, permissive).
48. AppArmor: принципы работы и сравнение с SELinux.
49. Мандатный контроль доступа в Linux: реализация и применение.
50. Безопасность сетевых сервисов ОС: SSH, FTP, SMB — рекомендации по настройке.
51. Защита от атак типа brute-force на учётные записи.
52. Настройка сложных политики паролей в Windows и Linux.
53. Двухфакторная аутентификация в ОС — возможности и инструменты.
54. Безопасность BIOS/UEFI: Secure Boot, защита от несанкционированной загрузки.
55. Роль UEFI и Secure Boot в защите ОС на этапе загрузки.
56. Защита от атак «холодной перезагрузки» (cold boot attack).
57. Управление правами доступа к файловой системе в Windows NT.
58. Управление правами в Linux: rwx, chmod, chown, umask.
59. Безопасность временных файлов и каталогов (/tmp, C:\Windows\Temp).
60. Анализ логов на предмет подозрительной активности: примеры.
61. Инструменты для мониторинга целостности файловой системы (например, AIDE, Tripwire).
62. Принципы безопасного удаления данных из ОС.
63. Роль централизованного управления (Active Directory, LDAP) в обеспечении безопасности.
64. Безопасность клиентских ОС в корпоративной сети.
65. Особенности защиты серверных ОС (Windows Server, Ubuntu Server).
66. Риски при использовании root-доступа в Linux и методы их минимизации.
67. Безопасность обновлений ПО: подпись пакетов, проверка источников.

68. Принципы безопасного размещения ОС в облаке (IaaS).
69. Анализ уязвимостей ОС с использованием сканеров (например, OpenVAS, Nessus).
70. Составление отчёта по результатам проверки защищённости ОС.

Тестовые задания для проведения промежуточной аттестации

1. Какая модель управления доступом реализована по умолчанию в большинстве дистрибутивов Linux?
   a) MAC
   b) DAC
   c) RBAC
   d) ABAC
2. Какой компонент Windows отвечает за проверку прав доступа к объектам?
   a) LSASS
   b) SAM
   c) Security Reference Monitor
   d) Winlogon
3. Что означает аббревиатура SELinux?
   a) Secure Enhanced Linux
   b) Security-Enhanced Linux
   c) System Enforcement Linux
   d) Standard Enterprise Linux
4. Какой механизм предотвращает выполнение кода из стека памяти?
   a) ASLR
   b) DEP
   c) SMEP
   d) CFG
5. Какая команда в Linux позволяет временно выполнять команды от имени root?
   a) su
   b) login
   c) sudo
   d) passwd
6. Какой уровень привилегий имеет ядро ОС на архитектуре x86?
   a) Ring 1
   b) Ring 2
   c) Ring 3
   d) Ring 0
7. Какой протокол используется для безопасного удалённого управления сервером в Linux?
   a) Telnet
   b) FTP

c) SSH
d) RDP

8. Что такое UAC в Windows?
   a) Служба шифрования дисков
   b) Механизм контроля учётных записей пользователей
   c) Фаервол
   d) Антивирус
9. Какой файл в Linux содержит хэши паролей пользователей?
   a) /etc/passwd
   b) /etc/group
   c) /etc/shadow
   d) /etc/sudoers
10. Какой атрибут куки в веб-приложениях предотвращает доступ к ней через JavaScript?
    a) Secure
    b) HttpOnly
    c) SameSite
    d) Domain
11. Какая технология шифрования дисков используется в Windows?
    a) LUKS
    b) VeraCrypt
    c) BitLocker
    d) EFS
12. Что такое TPM?
    a) Протокол передачи сообщений
    b) Доверенный платформенный модуль
    c) Тип файловой системы
    d) Средство аудита безопасности
13. Какой сервис в Linux отвечает за сбор системных логов по умолчанию в современных дистрибутивах?
    a) syslog
    b) rsyslog
    c) systemd-journald
    d) auditd
14. Какой журнал Windows содержит события входа пользователей?
    a) System
    b) Application
    c) Security
    d) Setup
15. Какая команда в Linux настраивает правила аудита файловых операций?
    a) logger
    b) auditctl
    c) journalctl
    d) logwatch
16. Что такое ASLR?

a) Механизм шифрования памяти
b) Случайное размещение библиотек и стека в памяти
c) Фильтр входящего трафика
d) Система управления пользователями

17. Какой инструмент в Windows позволяет ограничить запуск недоверенных программ?
a) UAC
b) AppLocker
c) Defender
d) Firewall

18. Какой стандарт используется для безопасной конфигурации ОС?
a) ISO 27001
b) NIST SP 800-53
c) CIS Benchmarks
d) GDPR

19. Какой фаервол по умолчанию используется в большинстве дистрибутивов Linux?
a) pfSense
b) Windows Defender Firewall
c) iptables / nftables
d) Cisco ASA

20. Что такое VM escape?
a) Выход из песочницы браузера
b) Атака, позволяющая выйти из виртуальной машины в хост-систему
c) Утечка данных через сеть
d) Взлом пароля root

21. Какой механизм изоляции используется в Docker для разделения процессов?
a) chroot
b) namespaces
c) sudo
d) ASLR

22. Что такое EFS в Windows?
a) Служба шифрования дисков
b) Служба шифрования отдельных файлов и папок
c) Система аудита
d) Механизм резервного копирования

23. Какой протокол обеспечивает безопасную загрузку ОС?
a) UEFI
b) Secure Boot
c) BIOS
d) GRUB

24. Какой тип RAID обеспечивает зеркалирование данных?
a) RAID 0
b) RAID 1

c) RAID 5
d) RAID 10

25. Какой из перечисленных — не метод защиты памяти?
a) DEP
b) ASLR
c) UAC
d) SMEP

26. Какой протокол передаёт данные без гарантии доставки?
a) TCP
b) UDP
c) HTTP
d) SSH

27. Какой порт использует протокол HTTPS по умолчанию?
a) 21
b) 22
c) 80
d) 443

28. Какой компонент Windows хранит учётные данные пользователей?
a) LSASS
b) SAM
c) SRM
d) CSRSS

29. Какой тип группы в Active Directory используется для предоставления доступа к ресурсам?
a) Глобальная
b) Универсальная
c) Локальная домена
d) Встроенные

30. Что делает команда chmod 700 file в Linux?
a) Делает файл доступным только владельцу
b) Делает файл общедоступным
c) Удаляет файл
d) Меняет владельца файла

31. Какой инструмент в Linux позволяет проверить, какие процессы слушают порты?
a) ping
b) netstat
c) ipconfig
d) route

32. Какой из перечисленных — не утилита для анализа сетевого трафика?
a) tcpdump
b) Wireshark
c) top
d) ss

33. Какой атрибут в AppArmor или SELinux определяет политику доступа?

a) ACL
b) Profile / Policy
c) SID
d) UID

34. Какой из перечисленных — не служба, которую рекомендуется отключать при харденинге?
a) Telnet
b) SSH
c) SMBv1
d) FTP

35. Что такое SIEM?
a) Система управления паролями
b) Система мониторинга и анализа событий безопасности
c) Антивирус
d) Механизм шифрования

36. Какой протокол используется для разрешения имён в IP-адреса?
a) DHCP
b) DNS
c) ARP
d) ICMP

37. Какой из перечисленных — не компонент подсистемы безопасности Windows?
a) LSASS
b) SAM
c) SRM
d) Nginx

38. Какой тип виртуализации использует гипервизор, работающий напрямую на «голом железе»?
a) Type 1
b) Type 2
c) Контейнеризация
d) Паравиртуализация

39. Какой механизм в Linux ограничивает системные вызовы в контейнере?
a) Capabilities
b) Seccomp
c) Cgroups
d) Namespaces

40. Какой из перечисленных — не метод шифрования данных в ОС?
a) BitLocker
b) LUKS
c) AppLocker
d) EFS

Критерии оценки для проведения зачета с оценкой по дисциплине (тестирование)

Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок.

Оценка	**Уровень сформированности компетенции**	**Критерии**
«Отлично» («зачтено»)	Высокий	Выполнено более 80% заданий предложенного теста
«Хорошо» («зачтено»)	Хороший	Выполнено 60-80% заданий предложенного теста
«Удовлетворительно» («зачтено»)	Достаточный	Выполнено 35-60% заданий предложенного теста
«Неудовлетворительно» («не зачтено»)	Недостаточный	Выполнено менее 35% заданий предложенного теста

Обновление оценочных материалов дисциплины

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____