Фонд оценочных средств для промежуточной аттестации

по дисциплине

Администрирование Windows

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Администрирование Windows**.
Семестр (семестры) изучения: 7 семестр.
Форма (формы) промежуточной аттестации: зачет 7 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Администрирование Windows» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	**Содержание компетенций согласно ФГОС (ОПОП ВО)**	**Индикаторы достижения компетенции согласно ОПОП**	**Перечень планируемых результатов обучения по дисциплине**
1	**2**	**3**	**4**
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах). УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах).	Знать: – основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий. Уметь: – составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов. Владеть: – иметь навыки вербальной коммуникации на техническом иностранном языке.
ОПК-12	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и	ОПК-12.1 Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные принципы конфигурирования и адми-	Знать: – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – понятие защиты информации, системы защиты; – основные виды угроз безопасности информации и их классификацию; – основные понятия, основные алгоритмы хранения и обработки данных

	системного программного обеспечения	нистрирования операционных систем. ОПК-12.2 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде. ОПК-12.3 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	ОС; – основные стандарты и алгоритмы передачи данных; – основные актуальные модели атак; – аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – требования к криптографическим системам защиты информации; – понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows. Уметь: – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами; – разрабатывать и конфигурировать программно-аппаратные средства защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет; – основами конфигурирования и разработки программно-аппаратных средств защиты информации, системы управления базами данных; компьютерных сетей, системы антивирусной защиты, средств криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	УК-4 ОПК-12	Раздел 1. Основные понятия и определения. 1.1. Основные понятия и определения. 1.2. Локальные политики безопасности 1.3. Парольная защита Windows 1.4. Использование средств защиты информации от несанкционированного доступа для усиления парольной защиты Windows	Лабораторная работа № 1	Вопросы к зачёту
2.	ОПК-12 УК-4	Раздел 2. Аудит в операционных системах Windows	Лабораторная работа № 2	Вопросы к зачёту
3.	ОПК-12 УК-4	Раздел 3. 3.1. Microsoft Active Directory	Лабораторная работа № 3	Вопросы к зачёту
		3.2. Microsoft Active Directory. Коллектор журналов	Лабораторная работа № 4	Вопросы к зачёту
4.	ОПК-12 УК-4	Раздел 4. 4.1. Positive Technologies MP SIEM. Активация, основные функции, сбор событий	Лабораторная работа № 5	Вопросы к зачёту
		4.2. Positive Technologies MP SIEM. Анализ защищенности	Лабораторная работа № 6	Вопросы к зачёту
		4.3. Positive Technologies MP SIEM. Обработка событий	Лабораторная работа № 7	Вопросы к зачёту

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2. Содержание оценочных средств

3.2.1. Содержание лабораторных работ

Лабораторная работа № 1 - Парольная защита в Windows

В виртуальной машине установить клиентскую операционную систему Windows.

С использованием локальных политик безопасности установить ограничения:

- минимальная длина пароля пользователя Windows – 14 символов;
- требование сложности пароля;
- блокировка учетной записи пользователя на 30 минут после пяти неудачных попыток авторизации.

Создать учетную запись пользователя Windows с паролем, удовлетворяющим установленным требованиям.

Сбросить пароль пользователя Windows с использованием предоставленного специализированного программного обеспечения.

Установить предоставленное средство защиты от несанкционированного доступа.

Сбросить пароль пользователя Windows на виртуальной машине с установленным средством защиты от несанкционированного доступа.

Настроить средство защиты от несанкционированного доступа для блокировки попыток сброса пароля специализированным ПО.

*Дистрибутивы, лицензии и специализированное программное обеспечение предоставляются преподавателем.

Лабораторная работа № 2 - Аудит в операционных системах Windows

Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:

- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;
- регистрация сведений об удалённых файлах.

Воссоздать структуру сети, сценарии использования компьютеров в локальной сети по результатам анализа предоставленных журналов безопасности, содержащую следующую информацию:

- сетевые имена компьютеров, входящих в локальную сеть;
- учётные записи пользователей и их соответствие сетевым именам компьютеров, на которых эти ученые записи используются;
- режим эксплуатации (время, дни недели) компьютеров;
- наличие сетевого программного обеспечения;
- определение наличия и типа контроллера домена Windows;
- используемые сетевые протоколы;
- используемое прикладное программное обеспечение;

- приблизительная схема локальной сети.

*специально подготовленные журналы, содержащие исходные события, предоставляются преподавателем

Лабораторная работа № 3 - Microsoft Active Directory

На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.

Клонировать виртуальную машину с серверной операционной системой, изменив идентификатор (SID) операционной системы и сетевое имя.

Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:

- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с исходной (по отношению к клонированной виртуальной машине с серверной операционной системой).

Серверной операционной системе добавить роль контроллера домена Active Directory.

Сконфигурировать контроллер домена с настройками по умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).

На клонированной виртуальной машине с серверной операционной системой настроить роль резервного контроллера домена (показатель успешности настройки – изменение структуры Active Directory на основном контроллере домена (добавление пользователей, компьютеров и т.д.) влечёт изменение структуры Active Directory на резервном контроллере домена.

Лабораторная работа № 4 - Microsoft Active Directory. Коллектор журналов

На двух виртуальных машинах установить соответственно серверную (Windows 2008 Server или более новая) и клиентскую (Windows 7 или более новая) операционные системы.

Настроить журналирование событий Windows – создать систему разграничения доступа (минимум два пользователя Windows с разным уровнем полномочий: полный доступ и доступ только для чтения) и настроить аудит использования привилегий для каталога на локальном диске и вложенных в него файлов, обеспечивающий регистрацию сведений:

- метод доступа к контролируемым файлам и каталогу;
- результат (успех, отказ) попытки использования привилегий;
- учетная запись пользователя, использующего привилегии;
- время события;

- регистрация сведений об удалённых файлах.

Между созданными виртуальными машинами настроить виртуальную сеть, соответствующую требованиям:

- все виртуальные машины находятся в одном virtual lan;
- все виртуальные машины имеют различные сетевые имена и ip-адреса;
- все виртуальные машины доступны друг другу по широковещательным рассылкам (находятся в одной подсети);
- основным шлюзом и сервером имён является виртуальная машина с серверной операционной системой.

Серверной операционной системе добавить роль контроллера домена Active Directory.

Сконфигурировать контроллер домена с настройками по-умолчанию, ввести клиентскую операционную систему в состав контроллера домена (показатель успешности настройки – на клиентской машине появляется возможность авторизоваться с доменной учетной записью).

Настроить коллектор (сборщик) журналов безопасности в серверной операционной системе для сбора событий из журнала безопасности клиентской операционной системы (показатель успешности выполнения задания - события по результатам аудита (в клиентской операционной системе, в журнале безопасности) доступа к каталогу, на основе созданной системы разграничения доступа, появляются в серверной операционной системе, в журнале коллектора (сборщика) журналов).

Лабораторная работа № 5 - Positive Technologies MP SIEM. Активация, основные функции, сбор событий

Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM. Активировать предоставленную лицензию, в соответствии с предоставленной документацией на Positive Technologies MP SIEM.

Создать задачу по сбору журналов из коллектора (сборщика) журналов Windows.

Создать задачу по сбору событий из базы данных Kaspersky Security Center.

Создать задачу по сбору событий по стандарту syslog.

Лабораторная работа № 6 - Positive Technologies MP SIEM. Анализ защищенности

Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM.

Провести поиск доступных хостов в сети. Выполнить задачу по сканированию доступных хостов на наличие уязвимостей в режиме PenTest (показатель успешности – обнаруженные уязвимости в результатах сканирования доступных хостов).

Проанализировать выявленные уязвимости рассмотреть, описать и принять меры по их устранению стандартными средствами Windows (закрытие портов, установка обновлений и т.д.).

Лабораторная работа № 7 - Positive Technologies MP SIEM. Обработка событий

Подключиться к удалённому стенду с установленным Positive Technologies MP SIEM.

Написать произвольное правило нормализации.

Написать произвольное правило агрегации.

Написать произвольное правило обогащения.

Написать произвольное правило корреляции.

Написать произвольное правило локализации.

3.2.2. Вопросы к зачёту

1. Модель OSI
2. Модель TCP/IP
3. Архитектура DNS
4. Протокол LDAP
5. MS Windows Server. Роли
6. MS Active Directory. Архитектура
7. MS Active Directory. Средства управления
8. Коллектор журналов событий Windows Server
9. Построение VPN сети средствами MS Windows Server
10. Настройка сервера удалённых рабочих столов RDP
11. Парольная защита Windows (локальная)
12. Система аудита Windows
13. RAID
14. UEFI/Legacy режимы загрузки Windows
15. SIEM-системы. Принципы построения и назначение
16. SIEM-системы. Формирование инцидентов и управление ими
17. SIEM-системы. Обработка событий
18. SIEM-системы. Настройка сбора событий

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

На зачёте студент получает билет. В билете два теоретических вопроса. На написание ответа дается 1 час. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-7	7x10=70
2	Зачет (теоретический вопрос)	2x10=20
	Итого	90

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса и лабораторной работы.
Максимальный балл – 10 баллов.

Отлично/зачтено/9-10 баллов	Хорошо/зачтено/7-8 баллов	Удовлетворительно/зачтено/5-6 баллов	Неудовлетворительно/не зачтено/0-4 балла
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Промежуточная аттестация в целом выставляется по результатам лабораторных работ и ответа на билет на зачете.

Критерий оценивания результатов зачета:

0 – 55 баллов – не зачет;

56 – 90 баллов – зачет.

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

Специальность 10.05.01 Компьютерная безопасность
Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Фонд оценочных средств по дисциплине «Администрирование Windows»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) А. Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1