МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

Рабочая программа дисциплины (модуля) «Безопасность операционных систем» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Клюев А.С., старший преподаватель, Кафедра информационной безопасности

Шумик Е.Г., кандидат экономических наук, доцент, Кафедра математики и моделирования, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от «____»_____20__г. , протокол № _____

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)
Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000BB70FC
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Безопасность в операционных системах» является формирование у студентов базовых навыков по применению методов защиты операционных систем и баз данных, дать студентам знания: различных аспектов, связанных с обеспечением безопасности операционных систем и баз данных, механизмов и сервисов безопасности компьютерных систем

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1к : Определяет законодательство Российской Федерации в области информационной безопасности и защиты информации; системы защиты государственной тайны; перечень сведений, относящихся к конфиденциальной информации и способы ее защиты;	РД1	Знание	основные определения и положения безопасности операционных систем, классификацию угроз и уязвимостей в существующих операционных системах, основные защитные механизмы операционных систем; программно-аппаратные средства защиты операционных систем;
			РД4	Знание	руководящие документы, регламентирующие безопасность операционных систем
	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.2к : владеет методами и средствами разграничения доступа к информационным ресурсам и умеет их реализовывать	РД2	Умение	четко классифицировать угрозы безопасности операционным системам
			РД3	Навык	практической работы со специализированным, прикладным программным обеспечением безопасности операционных систем

	ОПК-5.3 : Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;	ОПК-5.3.1к : тестирует систему безопасности на предмет ее уязвимости, отказоустойчивости и надежности	РД5	Умение	описать процесс принятия решения при выборе технологии; разрабатывать и внедрять модели обеспечения безопасности операционным системам; проводить протоколирование и аудит безопасности операционных систем четко классифицировать угрозы безопасности операционным системам
			РД6	Навык	применения стандартов и разработки политики безопасности операционных систем

2 Место дисциплины (модуля) в структуре ОПОП

Отнесение дисциплины к базовой части определяется особенностями взаимодействия ВГУЭС с рынком труда и региональными требованиями, выраженными в результатах образования и компетенциях.

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Информатика и основы программирования», «Операционные системы», «Основы информационной безопасности». На данную дисциплину опираются «Программно-аппаратные средства защиты информации».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	5	4	83	36	0	36	1	10	61	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Основные механизмы обеспечения безопасности	РД1, РД2, РД3, РД4, РД5, РД6	8	0	8	2	Тестовые задания, практические работы
2	Средства и методы аутентификации в ОС	РД1, РД2, РД3, РД4, РД5, РД6	8	0	8	2	Тестовые задания, практические работы
3	Разграничение доступа к ресурсам ОС	РД1, РД2, РД3, РД4, РД5, РД6	10	0	10	3	Тестовые задания, практические работы
4	Контроль работы подсистемы защиты	РД1, РД2, РД3, РД4, РД5, РД6	10	0	10	3	Тестовые задания, практические работы
Итого по таблице			**36**	**0**	**36**	**10**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Основные механизмы обеспечения безопасности.

Содержание темы: ОС Типовые угрозы безопасности ресурсов ОС. Требования к безопасности ОС. Основные группы механизмов защиты ресурсов ОС.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Средства и методы аутентификации в ОС.

Содержание темы: Аутентификация на основе пароля. Аутентификация с использованием физического объекта. Биометрические методы аутентификации. Многофакторная аутентификация. Технология SSO.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Разграничение доступа к ресурсам ОС.

Содержание темы: Классификация субъектов и объектов доступа. Права доступа. Методы разграничения доступа. Разграничение доступа к файловым объектам. Наследование разрешений. Разграничение доступа к устройствам. Ограничения на запуск программного обеспечения.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 4 Контроль работы подсистемы защиты.

Содержание темы: Организация и использование средств аудита. Контроль и восстановление целостности подсистемы защиты и ее параметров. Управление безопасностью ОС.

Формы и методы проведения занятий по теме, применяемые образовательные

технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

2. Потерпеев, Г. Ю. Сборник практических занятий для дисциплины безопасность операционных систем: Практикум : учебное пособие / Г. Ю. Потерпеев, О. В. Трубиенко, Д. П. Абрамов. — Москва : РТУ МИРЭА, 2023 — Часть 1— 2023. — 65 с. — ISBN 978-5-7339-1803-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/368750 (дата обращения: 28.02.2024). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Операционные системы : учебное пособие / сост. А. В. Калач, А. Н. Перегудов, В. В. Здольник. - Воронеж : Научная книга, 2022. - 92 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999933 (дата обращения: 26.02.2024).

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

· Компьютеры

Программное обеспечение:

· Microsoft Windows Server CAL 2008 Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

Специальность и специализация

10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2023

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1к : Определяет законодательство Российской Федерации в области информационной безопасности и защиты информации; системы защиты государственной тайны; перечень сведений, относящихся к конфиденциальной информации и способы ее защиты;
	ОПК-5.1 : Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;	ОПК-5.1.2к : владеет методами и средствами разграничения доступа к информационным ресурсам и умеет их реализовывать
	ОПК-5.3 : Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;	ОПК-5.3.1к : тестирует систему безопасности на предмет ее уязвимости, отказоустойчивости и надежности

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.1к : Определяет законодательство Российской Федерации в области информационной безопасности и защиты информации; системы защиты государственной тайны; перечень сведений, относящихся к конфиденциальной информации и способы ее защиты;	РД1	Знание	основные определения и положения безопасности операционных систем, классификацию угроз и уязвимостей в существующих операционных системах, основные защитные механизмы операционных систем ; программно- аппаратные средства защиты операционных систем;	ответы на тестовые задания
	РД4	Знание	руководящие документы, регламентирующие безопасность операционных систем	ответы на тестовые задания

Компетенция ОПК-5.1 «Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.1.2к : владеет методами и средствами разграничения доступа к информационным ресурсам и умеет их реализовывать	РД 2	Умение	четко классифицировать угрозы безопасности операционным системам	выполнение поставленных заданий
	РД 3	Навык	практической работы со специализированным, прикладным программным обеспечением безопасности операционных систем	выполнение поставленных заданий

Компетенция ОПК-5.3 «Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах;»

Таблица 2.3 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.3.1к : тестирует систему безопасности на предмет ее уязвимости, отказоустойчивости и надежности	РД 5	Умение	описать процесс принятия решения при выборе технологии; разрабатывать и внедрять модели обеспечения безопасности операционным системам; проводить протоколирование и аудит безопасности операционных систем четко классифицировать угрозы безопасности операционным системам	выполнение поставленных заданий
	РД 6	Навык	применения стандартов и разработки политики безопасности операционных систем	выполнение поставленных заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : основные определения и положения безопасности операционных систем, классификацию угроз и уязвимостей в существующих операционных системах, основные защитные механизмы операционных систем; программно- аппаратные средства защиты операционных систем;	1.1. Основные механизмы обеспечения безопасности	Тест	Экзамен в устной форме
		1.2. Средства и методы аутентификации в ОС	Тест	Экзамен в устной форме
		1.3. Разграничение доступа к ресурсам ОС	Тест	Экзамен в устной форме
		1.4. Контроль работы подсистемы защиты	Тест	Экзамен в устной форме
РД2	Умение : четко классифицировать угрозы безопасности операционным системам	1.1. Основные механизмы обеспечения безопасности	Лабораторная работа	Лабораторная работа
		1.2. Средства и методы аутентификации в ОС	Лабораторная работа	Лабораторная работа
		1.3. Разграничение доступа к ресурсам ОС	Лабораторная работа	Лабораторная работа
		1.4. Контроль работы подсистемы защиты	Лабораторная работа	Лабораторная работа
РД3	Навык : практической работы со специализированным, прикладным программным обеспечением безопасности операционных систем	1.1. Основные механизмы обеспечения безопасности	Лабораторная работа	Лабораторная работа
		1.2. Средства и методы аутентификации в ОС	Лабораторная работа	Лабораторная работа
		1.3. Разграничение доступа к ресурсам ОС	Лабораторная работа	Лабораторная работа
		1.4. Контроль работы подсистемы защиты	Лабораторная работа	Лабораторная работа
РД4	Знание : руководящие документы, регламентирующие безопасность операционных систем	1.1. Основные механизмы обеспечения безопасности	Тест	Экзамен в устной форме
		1.2. Средства и методы аутентификации в ОС	Тест	Экзамен в устной форме
		1.3. Разграничение доступа к ресурсам ОС	Тест	Экзамен в устной форме
		1.4. Контроль работы подсистемы защиты	Тест	Экзамен в устной форме
РД5	Умение : описать процесс принятия решения при выборе технологии; разрабатывать и внедрять модели обеспечения безопасности операционным системам; проводить протоколирование и аудит безопасности операци	1.1. Основные механизмы обеспечения безопасности	Лабораторная работа	Лабораторная работа
		1.2. Средства и методы аутентификации в ОС	Лабораторная работа	Лабораторная работа
		1.3. Разграничение доступа к ресурсам ОС	Лабораторная работа	Лабораторная работа

	онных систем четко классифицировать угрозы безопасности операционным системам	1.4. Контроль работы подсистемы защиты	Лабораторная работа	Лабораторная работа
РД6	Навык : применения стандартов и разработки политики безопасности операционных систем	1.1. Основные механизмы обеспечения безопасности	Лабораторная работа	Лабораторная работа
		1.2. Средства и методы аутентификации в ОС	Лабораторная работа	Лабораторная работа
		1.3. Разграничение доступа к ресурсам ОС	Лабораторная работа	Лабораторная работа
		1.4. Контроль работы подсистемы защиты	Лабораторная работа	Лабораторная работа

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-4	Лабораторная работа	Экзамен	Итого
Лекционные занятия	30			30
Лабораторные занятия		50		50
Промежуточная аттестация			20	20
Итого	30	50	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1. Какое из перечисленных программных средств может применяться для обеспечения двухфакторной аутентификации в операционной системе?

DeviceLock

Process Explorer

JaCarta SecurLogon

Adobe Photoshop

2. Какой фактор аутентификации не применяется в eToken, но встречается в некоторых моделях JaCarta?

Пароль

Физический объект

Биометрия

Все применяются

3. Какая файловая система должна быть на диске, к ресурсам которого необходимо присвоить категорию конфиденциальности в Secret Net?

exFAT

UDF

NTFS

FAT32

4. Какой из параметров не учитывается при внесении устройства в белый список в DeviceLock?

Идентификатор продукта

Идентификатор производителя

Страна изготовитель

Серийный номер

5. Под каким уровнем конфиденциальности необходимо войти в систему администратору, чтобы Secret Net позволила ему изменять параметры операционной системы?

Высший (строго конфиденциально)

Средний (конфиденциально)

Низший (не конфиденциально)

Администратору можно проводить настройки под любым уровнем

6. С помощью чего можно настроить доступность функционала таких приложений как eToken PKI Client для пользователей?

Реестр

Командная строка

Административные шаблоны

Настройки приложения

7. Какая информация не содержится в профиле, создаваемом на eToken для входа в операционную систему?

Домен

Логин

Пин-код

Пароль

8. Какая из моделей разграничения доступа не применяется в Secret Net?

30264

Дискреционная модель

Мандатная модель

Ролевая модель

Применяются все перечисленные модели

9. Какую возможность предоставляет использование технологии SSO?

Развитие и продвижение сайта

Безопасное подключение к web-ресурсам

Автоматическая аутентификация в приложениях при подключенном eToken

Передача электронной почты в сети

10. Каким образом предоставить полный доступ для любой клавиатуры, подключенной к системе с установленным запретом доступа к usb-портам в DeviceLock?

Внести клавиатуру в белый список как Unique Device

Внести клавиатуру в белый список как Device Model

Отключить управление доступом к USB HID в настройках безопасности программы

Любой из перечисленных вариантов

11. Какую оснастку необходимо добавить в консоль управления, чтобы провести анализ безопасности операционной системы?

Монитор IP-безопасности

Системный монитор

Анализ и настройка безопасности

Редактор объектов групповой политики

12. Какое действие не фиксируется при аудите системных событий?

Запуск элементов системы безопасности

Отключение элементов системы безопасности

Присвоение привилегий пользователю

Изменение системного времени

13. Какие события не фиксируются при аудите управления учетными записями?

Создание учетной записи для пользователя

Изменение пароля пользователя

Назначение прав пользователю

Внесение учетной записи в группу

14. Какие типы объектов не могут подвергаться фиксации при аудите доступа к объектам?

Файл

Каталог

Учетная запись

Ключ реестра

15. В результате какого действия программа, запрещенная правилом хеша, будет запущена?

Программу перенесли в другую папку

Программу переименовали

Программу изменили или заменили на другую версию

Программу разрешили правилом сертификата

16. С помощью какого правила в политике ограниченного использования программ можно запретить запуск любых приложений от одного производителя?

Правилом пути

Правилом хеша

Правилом сертификата

Правилом зон интернета

17. Отсутствие настройки по какому параметру может привести к бесполезности параметра

«Требовать неповторяемости паролей»?

Максимальный срок действия пароля

Минимальная длина пароля

Минимальный срок действия пароля

Пароль должен отвечать требованиям сложности

18. Чем обусловлено требование неповторяемости паролей?

Пароль не должен повторять логин пользователя

У всех пользователей должны быть разные пароли

Пароль должен отличаться от нескольких предыдущих

В пароле не должно быть одинаковых сегментов

19. Какого типа журнала аудита в DeviceLock не существует?

Журнал событий

Журнал событий и DeviceLock

Журнал теневого копирования

Журнал DeviceLock

20. Какой тип аудита в DeviceLock фиксирует все попытки доступа, которые были заблокированы?

Аудит успеха

Аудит разрешений

Аудит запрета

Аудит отказа

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 4 темам на лекционных занятиях, в каждом тесте 11 вопросов

Шкала оценки

Оценка	Баллы	Описание
5	4	Студент не допустил ошибок
4	3	Студент совершил от 2 до 4 ошибок в ответах на тест
3	2	Студент совершил от 5 до 7 ошибок в ответах на тест
2	1	Студент совершил 8 и более ошибок в ответах на тест

5.2 Пример заданий на лабораторную работу

Лабораторная работа №1 Восстановление ОС Windows

Целью данной работы является изучение методики восстановления ОС «Windows», освоение практических навыков восстановления работоспособности ОС, технологии восстановления операционной системы после сбоя с помощью загрузочного диска Hiren.

Планируемые результаты обучения в соответствии с компетенцией: ПК-4, ПК-11 перечисленные и описанные в РПД к данной дисциплине.

Содержание лабораторной работы:

1. Попробуйте запустить 1-ю виртуальную машину в обычном режиме с помощью программы VMware Player.

2. Восстановление boot.ini

3. Восстановление MBR

4. Сброс пароля

5. Штатные средства восстановления

Краткие методические указания

На выполнение одной лабораторной работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме.

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.

2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/или н еверно применил методы необходимые его выполнения.