МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
24 марта 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «Б1.В.02 МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2025

Срок получения образования: 2 года

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2025

Разработчики:
Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.10.2024, № 10-24

Содержание

1. Цель и задачи освоения дисциплины (модуля)

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

3. Место дисциплины в структуре ОП

4. Объем дисциплины и виды учебной работы

5. Содержание дисциплины
   5.1. Разделы, темы дисциплины и виды занятий
   5.2. Содержание разделов, тем дисциплины и формы текущего контроля

6. Оценочные материалы текущего контроля

7. Оценочные материалы промежуточной аттестации

8. Порядок проведения промежуточной аттестации

9. Материально-техническое и учебно-методическое обеспечение дисциплины
   9.1. Перечень основной и дополнительной учебной литературы
   9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
   9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
   9.4. Оборудование и технические средства обучения

10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - сформировать способность описывать и проверять правила управления доступом и информационными потоками, выбирать подходящую модель безопасности и связывать требования защиты с настройкой и проверкой механизмов компьютерных систем.

Задачи изучения дисциплины:

- освоить субъект-сущностное представление системы, графы доступа и сравнение меток безопасности;
- научиться применять дискреционные, мандатные и ролевые правила к коротким профессиональным ситуациям;
- освоить описание состояний, переходов и информационных потоков, выявление простых контрпримеров к свойствам безопасности;
- получить опыт проверки МКЦ и совместного действия механизмов доступа в учебной Astra Linux;
- научиться формулировать проверяемые требования и политики защиты, сопоставлять модель с реализацией и включать проверки безопасности в жизненный цикл ПО.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-1 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.1 Разрабатывает профили защиты компьютерных систем

Знать:

ПК-1.1/Зн1 Теоретические основы угроз безопасности информации

ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных

Уметь:

ПК-1.1/Ум1 Разрабатывать политики безопасности, основываясь на анализе потребностей организации и действующих угроз

ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы

Владеть:

ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей

Знать:

ПК-1.2/Зн1 Особенности разработки модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/Зн2 Принципы построения модели безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

Уметь:

ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.2/Ум2 Уметь применять стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

Владеть:

ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

ПК-1.2/Нв2 Владеть навыками применения стандартов в области информационной безопасности при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.02 «Модели безопасности компьютерных систем» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
4 семестр	144	4	32	32	44	Экзамен (36)
Всего	144	4	32	32	44	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	его	кционные занятия	актические занятия	остоятельная работа	анируемые результаты чения, соотнесенные с ультатами освоения ограммы

	Все	Ле	Пр	Са	Пла обу рез про
Раздел 1. Основные понятия и определения в области моделирования безопасности компьютерных систем	**14**	**4**	**4**	**6**	ПК-1.1 ПК-1.2
Тема 1.1. Элементы теории графов. Модель решётки	14	4	4	6	
Раздел 2. Модели компьютерных систем с дискреционным управлением доступом	**16**	**4**	**6**	**6**	ПК-1.1 ПК-1.2
Тема 2.1. Модели ХРУ и ТМД. Классическая модель Take-Grant. Расширенная модель Take-Grant	16	4	6	6	
Раздел 3. Модели компьютерных систем с мандатным управлением доступом	**20**	**6**	**6**	**8**	ПК-1.1 ПК-1.2
Тема 3.1. Классическая модель Белла—ЛаПадулы. Модель Биба. Модель СВС	20	6	6	8	
Раздел 4. Модели безопасности информационных потоков	**14**	**4**	**4**	**6**	ПК-1.1 ПК-1.2
Тема 4.1. Модель изолированной программной среды. Автоматная, программная и вероятностная модели безопасности информационных потоков	14	4	4	6	
Раздел 5. Модели компьютерных систем с ролевым управлением доступом	**16**	**6**	**4**	**6**	ПК-1.1 ПК-1.2
Тема 5.1. Модели ролевого управления доступом: иерархия ролей, механизм ограничений. Модель администрирования ролевого управления доступом	16	6	4	6	
Раздел 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)	**14**	**4**	**4**	**6**	ПК-1.1 ПК-1.2
Тема 6.1. Дискреционные ДП-модели. МРОСЛ ДП-модель	14	4	4	6	
Раздел 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем	**14**	**4**	**4**	**6**	ПК-1.1 ПК-1.2

Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition	14	4	4	6	
Итого	**108**	**32**	**32**	**44**	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Основные понятия и определения в области моделирования безопасности компьютерных систем

Тема 1.1. Элементы теории графов. Модель решётки

Понятие и классификация угроз безопасности информации. Понятие и основные виды политик безопасности управления доступом и информационными потоками. Сущность, субъект, доступ, информационный поток. Утечка права доступа и нарушение безопасности компьютерных систем. Математические основы моделей безопасности.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 2. Модели компьютерных систем с дискреционным управлением доступом

Тема 2.1. Модели ХРУ и ТМД. Классическая модель Take-Grant. Расширенная модель Take-Grant

Модель матрицы доступов Харрисона–Руззо–Ульмана (ХРУ): описание модели, анализ безопасности. Модель типизированной матрицы доступов (ТМД). Модель распространения прав доступа Take-Grant: основные положения, классическая и расширенная модель Take-Grant. Представление систем Take-Grant системами ХРУ.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 3. Модели компьютерных систем с мандатным управлением доступом

Тема 3.1. Классическая модель Белла—ЛаПадулы. Модель Биба. Модель СВС

Модель Белла-ЛаПадулы: классическая модель, политика low-watermark, безопасность переходов. Недостатки модели Белла-ЛаПадулы, примеры реализации запрещённых информационных потоков. Модель мандатного контроля целостности информации Биба. Модель систем военных сообщений. Практическая интерпретация МКЦ и административных полномочий в Astra Linux по лабораторной работе 6; разграничение конфиденциальности и целостности.

Текущий контроль

Вид (форма) контроля
Тестирование
Практическая работа

Раздел 4. Модели безопасности информационных потоков

Тема 4.1. Модель изолированной программной среды. Автоматная, программная и вероятностная модели безопасности информационных потоков

Субъектно-ориентированная модель изолированной программной среды. Автоматная модель безопасности информационных потоков. Программная модель контроля информационных потоков. Вероятностная модель безопасности информационных потоков.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 5. Модели компьютерных систем с ролевым управлением доступом

Тема 5.1. Модели ролевого управления доступом: иерархия ролей, механизм ограничений. Модель администрирования ролевого управления доступом

Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Модель мандатного ролевого управления доступом.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)

Тема 6.1. Дискреционные ДП-модели. МРОСЛ ДП-модель

Элементы состояния и правила преобразования состояний системы в рамках базовой ДП-модели. ДП-модели без кооперации доверенных и недоверенных субъектов. Иерархическое представление мандатной сущностно-ролевой ДП-модели управле-ния доступом и информационными потоками в операционных системах семейства Linux. Связь модели с файловой иерархией и уровнями целостности Astra Linux; лабораторная работа 7.

Текущий контроль

Вид (форма) контроля
Практическая работа

Раздел 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем

Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition

Модели управления доступом, реализованные в современных ОС, СУБД и других компьютерных системах. Проблемы адекватности формальных моделей управления доступом условиям функционирования реальных компьютерных систем. Вопросы верификации корректности реализации формальных моделей управления. Примеры и особенности реализации моделей управления доступом и информационными потоками в отечественных защищенных ОС. Практическая проверка совместного действия мандатных и дискреционных механизмов Astra Linux по лабораторной работе 8. DevOps и DevSecOps: версии исходников, этапы CI/CD, инфраструктура как код, включение проверок безопасности в жизненный цикл. Прослеживаемость от требования политики к проверке и решению о выпуске.

Текущий контроль

Вид (форма) контроля
Практическая работа

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 4 семестр.

Промежуточная аттестация по дисциплине проводится в форме экзамена. Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:

Экзамен оценивается по пятибалльной шкале:

- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы

правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

7. Оценочные материалы текущего контроля

Раздел 1. Основные понятия и определения в области моделирования безопасности компьютерных систем
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 1.1. Элементы теории графов. Модель решётки

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Объекты, субъекты и угрозы геосервиса

Для учебного геосервиса с закрытым слоем, редактором и читателем выделить процессы-субъекты, защищаемые объекты и операции. Описать по одному случаю нарушения конфиденциальности, целостности и доступности и связать их с понятными правилами защиты.

2. Граф доступа и решетка меток

По условию Н < С < В построить схему уровней и определить точные верхнюю и нижнюю грани пар Н/С и С/В. Для отдельного графа А → Б → В показать достижимость В из А и объяснить различие пути и непосредственного ребра.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Сначала нужно определить защищаемый объект, затем нежелательное событие и правило, препятствующее ему. Упорядочьте действия.

А. Сформулировать правило защиты
Б. Описать нежелательное событие
В. Выбрать защищаемый объект

2. Постройте граф по списку связей: сначала создают вершины, после этого наносят стрелки и проверяют схему.

А. Нанести все вершины
Б. Сверить граф со списком связей
В. Добавить заданные стрелки

3. Нужно найти путь А → Б → В. Исходное положение — А; каждый переход идет по указанной стрелке.

А. Перейти по стрелке А → Б
Б. Перейти по стрелке Б → В
В. Зафиксировать достижение В
Г. Начать в А

4. Правило разрешает запись только редактору. В модели запись доступна читателю. Сначала фиксируют нарушение, затем исправляют правило и повторяют проверку.

А. Повторить проверку записи читателем
Б. Зафиксировать новый результат
В. Исправить ошибочное разрешение
Г. Зафиксировать доступ читателя на запись

Раздел 2. Модели компьютерных систем с дискреционным управлением доступом
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 2.1. Модели ХРУ и ТМД. Классическая модель Take-Grant. Расширенная модель Take-Grant

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Матрица разрешений учебного хранилища

Для хранилища с двумя файлами и ролями читателя, редактора и ответственного составить матрицу доступа конкретных пользователей. Задать необходимые права read/write, проверить один разрешенный и один запрещенный запрос и обосновать отсутствие лишних прав.

2. Передача права в учебном графе Take-Grant

Использовать выданное правило: А может получить read к F от Б при наличии соответствующего разрешения take, а затем передать свое read В при разрешении grant. Построить начальный граф и два последовательных преобразования; отдельно объяснить, почему передача до получения права не выполняется.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Проверьте доступ по матрице: субъект и объект уже известны, решение принимают по найденной ячейке.

А. Выдать решение
Б. Выбрать строку субъекта
В. Найти в ней столбец объекта
Г. Проверить наличие нужного права

2. У Анны нет read к F. Команда выдает это право, после чего Анна читает F. Упорядочьте состояния и действие.

А. Состояние с read
Б. Выполнение команды выдачи read
В. Чтение F по полученному праву
Г. Исходное состояние без read

3. Проверка отзыва права начинается со снимка исходной ячейки. Затем право удаляют и проверяют повторный запрос.

А. Повторить запрос
Б. Зафиксировать исходное право
В. Удалить право из ячейки
Г. Проверить отказ

4. В задаче А получает read от Б, а затем передает его В. До получения А не может передать это право. Упорядочьте действия.

А. Передать read от Б к А

Б. Проверить наличие read у Б и разрешенность передачи
В. Передать read от А к В
Г. Проверить наличие read у А

5. Матрица после команды не совпала с ожидаемой. Сначала сохраняют оба состояния, затем находят различие и проверяют правило команды.

А. Сохранить исходную и полученную матрицы
Б. Объяснить или исправить расхождение
В. Найти измененную ячейку
Г. Сопоставить изменение с правилом команды

Раздел 3. Модели компьютерных систем с мандатным управлением доступом
Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 3.1. Классическая модель Белла—ЛаПадулы. Модель Биба. Модель СВС

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Политика конфиденциальности по уровням

Для субъектов уровней 1 и 2 и объектов тех же уровней составить таблицу чтения и записи по учебным правилам «чтение не вверх, запись не вниз», рассматривая запись без чтения и считая остальные разрешения выданными. Объяснить один разрешенный и один запрещенный поток.

2. Сопоставление конфиденциальности и целостности

Сравнить учебные правила Белла—ЛаПадулы «не читать вверх, не писать вниз» и строгие правила Биба «не читать вниз, не писать вверх» для двух уровней и операции записи без чтения. Подобрать по одному запросу, который различается по решению, и объяснить разные цели политик.

3. Уровни и категории доступа

Задать метки закрытых документов как пару «уровень, набор категорий». Для чтения использовать условие: уровень субъекта не ниже объекта и все категории объекта входят в категории субъекта. Проверить четыре выданные пары меток и пояснить отказ при отсутствии одной категории.

4. МКЦ и административные действия в Astra Linux

По ЛР 6 в выделенной учебной ВМ сравнить выполнение предусмотренной административной операции в сессиях с разными уровнями целостности. Перед изменениями зафиксировать состояние МКЦ, после изменения повторить наблюдение. Объяснить, почему наличие административных прав не отменяет мандатных условий.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Проверка чтения по меткам выполняется в заданном порядке: сначала уровень, затем категории, затем итог.

А. Проверить включение нужных категорий
Б. Сравнить уровни субъекта и объекта
В. Принять решение по двум условиям

2. В учебной работе состояние МКЦ проверяют до изменения, после включения повторяют проверку.

А. Узнать текущее состояние МКЦ
Б. Повторно проверить состояние
В. Записать результат
Г. Включить МКЦ в разрешенной учебной среде

3. В условной политике запись разрешена при целостности субъекта не ниже объекта. Сначала получают метку субъекта, затем объекта; после этого сравнивают их.

А. Выдать решение

Б. Определить уровень целостности объекта
В. Определить уровень целостности субъекта
Г. Сравнить уровни по заданному правилу

4. Нужно проверить запрет чтения вверх без изменения других условий. Сначала задают метки, затем выполняют запрос и сравнивают результат с правилом.

А. Зафиксировать решение
Б. Сопоставить решение с политикой
В. Выполнить запрос чтения
Г. Назначить субъекту и объекту уровни из задания

Раздел 4. Модели безопасности информационных потоков

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 4.1. Модель изолированной программной среды. Автоматная, программная и вероятностная модели безопасности информационных потоков

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Путь информационного потока

Построить схему «закрытый файл — процесс — открытый файл» для двух операций чтения и записи. Указать источник и получателя на каждом шаге, обнаружить недопустимую передачу по заданному запрету и предложить точку контроля.

2. Проверка свойства автоматной модели

Для автомата с состояниями «нет доступа», «чтение», «запись» задать переходы по запросам читателя и редактора. Проверить свойство «читатель не достигает состояния записи» перебором всех переходов этого малого автомата; при ошибке показать контрпример.

3. Открытый вывод и скрытый вход

На двух простых функциях — вывод постоянной строки и вывод строки, зависящей от секретного бита — сравнить публичный результат при неизменных открытых входах. Объяснить найденную зависимость и границы вывода; дополнительно обсудить влияние задержки, если она не включена в модель.

Раздел 5. Модели компьютерных систем с ролевым управлением доступом

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 5.1. Модели ролевого управления доступом: иерархия ролей, механизм ограничений. Модель администрирования ролевого управления доступом

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Роли для согласования публикаций

Для процесса подготовки и одобрения публикации геосервиса определить роли читателя, редактора и согласующего, назначить им необходимые разрешения и связать с пользователями. Подготовить проект политики и проверить два разных пользовательских сценария.

2. Иерархия и ограничения ролей

Задать роль старшего редактора, наследующую просмотр и добавляющую редактирование. Ввести запрет одобрения собственного документа. Показать итоговые права и проверить, не отменяет ли наследование установленное ограничение.

Раздел 6. Модели безопасности управления доступом и информационными потоками (ДП-модели)

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 6.1. Дискреционные ДП-модели. МРОСЛ ДП-модель

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Состояние и правило ДП-модели

Для небольшого учебного примера явно перечислить субъекты, сущности, разрешенные доступы и возникающие потоки. Описать правило чтения: предусловие, изменение состояния и направление потока; проверить случай с выполненным и невыполненным предусловием.

2. Иерархия целостности файловой системы Astra Linux

По ЛР 7 на учебной ВМ создать выданную иерархию каталогов и файлов и проверить правило соотношения уровней целостности родителя и дочерних сущностей. Зафиксировать отказ при несогласованных метках и выполнить согласованное изменение уровней, сохранив протокол.

3. Требования к модели защиты

Для учебного хранилища пространственных данных описать назначение, защищаемые данные, угрозы и предполагаемую среду. Сопоставить каждой угрозе правило доступа или потока и наблюдаемый способ проверки. Оформить содержательный проект профиля защиты без заявления о сертификации.

Раздел 7. Примеры реализации и основные направления развития формальных моделей безопасности компьютерных систем

Контролируемые ИДК: ПК-1.1 ПК-1.2

Тема 7.1. Модели управления доступом в ОС Windows. Модели управления доступом в ОС семейства Linux. Вопросы верификации формальных моделей управления доступом и корректности их реализации. Модель управления доступом в отечественной ОС Astra Linux Special Edition

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Совместная проверка мандатного и дискреционного доступа

По ЛР 8 в Astra Linux организовать работу двух учебных пользователей с файлами. Выбрать случай отказа из-за обычных прав и случай отказа из-за мандатных атрибутов; для каждого записать условия, запрос, результат и объяснение по политике.

2. Проверки безопасности в конвейере разработки

По лекциям DevOps и DevSecOps изобразить учебный конвейер от выбранной версии кода до развертывания. Разместить проверки исходников, подготовленного артефакта и работающего сервиса; задать условие остановки выпуска и порядок повторной проверки после исправления.

3. Модель и фактическая реализация политики

Для одного правила доступа из выполненных заданий составить набор разрешенных и запрещенных запросов, выполнить их на учебной реализации и сопоставить ответы со спецификацией. Обнаруженное различие объяснить, исправить в согласованных границах и повторить проверку.

8. Оценочные материалы промежуточной аттестации

4 семестр, Экзамен

Контролируемые ИДК: ПК-1.1 ПК-1.2

Вопросы/Задания:

1. Чем субъект отличается от объекта доступа?

2. В чем различие ребра и пути графа?

3. Для чего в модели нужна политика безопасности?

4. Что означает точная верхняя грань пары в заданной цепочке уровней?

5. Почему нужно явно задавать границы модели?

6. Как по матрице проверить разрешение операции?

7. Что изменяет команда выдачи права в учебной модели матрицы?

8. Зачем тип объекта включают в условие команды?

9. Чем передача права отличается от выполнения разрешенной операции?

10. Почему начальная матрица без лишних прав еще не доказывает безопасность?

11. Какое свойство защищает классическая модель Белла—ЛаПадулы?

12. Чем направленность строгих правил Биба отличается от правил конфиденциальности?

13. Для чего наряду с уровнем используют категории?

14. Почему для административной операции проверяют уровень целостности процесса?

15. Что должно оставаться истинным после безопасного перехода модели?

16. Куда направлен поток при записи процессом данных в файл?

17. Чем временной канал отличается от передачи через содержимое файла?

18. Что проверяет условие невлияния секретного входа на публичный выход?

19. Почему одинаковые результаты двух запусков не являются общим доказательством?

20. Как вероятность публичного ответа может зависеть от закрытой информации?

21. Какие сущности связывает базовая ролевая модель?

22. Для чего используется иерархия ролей?

23. Какое ограничение выражает запрет автору окончательно одобрять собственный документ?

24. Почему роль, назначенная пользователю, и роль, активированная в сессии, не всегда одно и то же?

25. Что проверяют после отзыва роли?

26. Чем право доступа отличается от информационного потока в описании ДП-модели?

27. Что нужно указать в правиле преобразования состояния?

28. Как соотносятся уровни целостности каталога и вложенных сущностей по ЛР 7?

29. Почему понижение уровня родителя требует проверки дочерних сущностей?

30. Что показывает контрпример к свойству модели?

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. - Издательский центр "Академия", 2005. - 144 - 5-7695-2053-1. - Текст: непосредственный.

2. Богульская Н. А. Модели безопасности компьютерных систем: учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск: СФУ, 2019. - 206 с. - 978-5-7638-4008-7. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/157578 - Режим доступа: по подписке

Дополнительная литература

1. Мызникова Т. А. Основы работы в операционной системе Astra Linux: учебно-методическое пособие к выполнению лабораторных работ / Т. А. Мызникова, Д. А. Елизаров. - Омск: ОмГУПС, 2024. - 33 с. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/505051 - Режим доступа: по подписке

2. Влацкая И. В. Безопасное администрирование Astra Linux SE: учебное пособие / И. В. Влацкая, И. А. Щудро, Д. А. Мусалимов. - Оренбург: ОГУ, 2024. - 186 с. - 978-5-7410-3326-5. - Текст: электронный // Издательство Лань: [сайт]. - URL: https://e.lanbook.com/book/502709 - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. https://intuit.ru/ - Электронная образовательная среда "ИНТУИТ"
2. https://urait.ru - Образовательная платформа «Юрайт»
3. https://rusneb.ru/ - Национальная электронная библиотека (НЭБ)
4. https://e.lanbook.com/ - Электронная библиотечная система "Лань"
5. https://www.elibrary.ru/ - НЭБ eLIBRARY

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
1. Sublime Text 3;
2. 7Zip;
3. Microsoft Office;
4. Notepad++;
5. Microsoft Visual Studio;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс
Маркерная доска - 0 шт.
Моноблок - 64 шт.
Проектор - 5 шт.
Автоматизированное рабочее место (АРМ) - 15 шт.
Доска настенная одноэлементная - 2 шт.

Учебная аудитория
Автоматизированное рабочее место (АРМ) - 1 шт.
Проектор - 2 шт.
Доска настенная одноэлементная - 1 шт.

Смешанный тип
Автоматизированное рабочее место (АРМ) - 1 шт.
Доска настенная одноэлементная - 2 шт.
Интерактивная панель - 1 шт.
Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития,

индивидуальных возможностей и состояния здоровья таких обучающихся.