МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине
«МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2025

ВВЕДЕНИЕ

1. Цель и задачи изучения дисциплины

Целью преподавания дисциплины «Методы оценки безопасности компьютерных систем» является раскрытие основы технических средств, используемых в компьютерной индустрии для защиты информации, теоретические модели защиты информации, практическое их применение в современных компьютерных системах, а также приобретение студентами знаний по техническому обеспечению защиты информации и формирование практических навыков работы.

В результате освоения дисциплины студенты должны:

Знать:

- суть системного подхода к построению высоконадежных ИС;
- углубить знания в области теории надёжности;
- изучить инженерные методы решения задач оценки надежности, точности, качества функционирования ИС.

2. Оборудование и материалы

Аппаратные средства: персональный компьютер;

Программные средства Альт Рабочая станция 10, Альт Рабочая станция К, Альт «Сервер», Пакет офисных программ - Р7-Офис.

Учебный класс оснащен IBM-совместимыми компьютерами, объединенными в локальную сеть. Локальная сеть учебного класса имеет постоянный доступ к сети Internet по выделенной линии. Для проведения лабораторных работ необходимо следующее программное обеспечение: операционная система Альт Рабочая станция, пакет офисных программ Р7-Офис.

3. Наименование практических работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
4 семестр			
1	Практическая работа 1. Содержание и основные понятия компьютерной безопасности	4	4
1	Практическая работа 2 Угрозы безопасности в компьютерных системах	4	4
2	Практическая работа 3. Политика и модели безопасности в компьютерных системах	4	4
2	Практическая работа 4. Модели безопасности на основе дискреционной политики	4	4
2	Практическая работа 5. Модели безопасности на основе мандатной политики	4	4
3	Практическая работа 6. Модели безопасности на основе тематической политики	4	4
3	Практическая работа 7. Модели безопасности на основе ролевой политики	4	4
4	Практическая работа 8. Автоматные и теоретико-вероятностные модели информационного невлияния и информационной	4	4

	невыводимости		
4	Практическая работа 9. Модели и механизмы обеспечения целостности данных	4	4
	Итого за 4 семестр	**36**	**36**

4. Содержание лабораторных работ

Тема 1. Содержание и основные понятия компьютерной безопасности

История развития теории и практики обеспечения компьютерной безопасности.

Понятия "информационная безопасность" и компьютерная безопасность. Безопасность информации в компьютерных системах и ее составляющие - конфиденциальность, целостность и правомерная доступность (сохранность) информации.

Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности. Общие принципы обеспечения компьютерной безопасности.

Систематика методов и механизмов обеспечения компьютерной безопасности.

Методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность информации — разграничение доступа к данным, контроль, управления информационной структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭЦП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти.

Методы и механизмы общеархитектурного характера — идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями.

Методы и механизмы инфраструктурного характера — управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей.

Методы и механизмы обеспечивающего (профилактирующего) характера — протоколирование и аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативно-организационная регламентация использования КС, обучение, нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности КС.

Тема 2. Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах.

Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация","категорирование" и "каталогизация".

Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации

— критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединенияклассов).

Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным имеждународным стандартам.

Идентификация и спецификация (описание) угроз — выявление угрозы определенного типа иприсвоение ей уникального идентификатора, определение и описания источника

(природы) угрозы, активов/объектов, подверженных воздействию угрозы, способов и особенностейреализации/осуществления.

Общая схема оценивания угроз — оценка [вероятности] реализации угрозы и оценка ущерба от реализации угрозы. Оценка рисков, методы и шкалы оценки. Методы экспертной оценки вероятности реализации и/или степени опасности угроз.

Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

Тема 3. Политика и модели безопасности в компьютерных системах

Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно- алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС.

Составляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС.

Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.

Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы. Понятие субъекта и объекта, потока информации и доступа субъекта к объекту, методов и прав доступа, разграничения доступа.

Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временная,маршрутная.

Программно-техническая структура компьютерной системы в контексте безопасности. Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений).

Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств). Модель и теоремы гарантирования безопасности (по Щербакову). Изолированная программная среда.

Тема 4. Модели безопасности на основе

дискреционной политики

Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект.

Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.

Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры.

Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы

объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX) и децентрализованная структура (списки доступа объектов в ОС Windows).

Модель распространения прав доступа Харисона-Руззо-Ульмана. Примитивные операции и команды изменения матрицы доступа. Монотонные, монооперационные и одноусловные системы. Теорема безопасности Харисона-Руззо-Ульмана для монооперационных систем и в

общем случае. Троянские программы. Сценарий атаки троянской программой в нотации модели Харисона- Руззо-Ульмана.

Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ. Типы субъектов и объектов. Родительские и дочерние типы. Графотношений (порождений) наследственности. Теорема безопасности для ацикличных реализаций систем на основе типизованной матрицы доступа.

Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системахс добровольным управлением доступом. Специфичные права субъектов доступа *take* и *grant.* Граф доступа. Примитивные операции (команды), изменяющие состояние графа доступа. tg-связность вершин графа доступа,"острова" и "мосты" в графе доступа. Условия и теорема возможности санкционированного получения субъектом прав доступа на какой-либо объект. Условия и теорема возможности несанкционированного получения субъектом прав доступа на какой-либо объект ("похищения" прав доступа).

Расширенная (extended) модель TAKE-GRANT. Неявные (вероятностные) каналы утечки информации и "мнимые" дуги в графе доступов. Примитивные (элементарные) команды преобразования графа доступов для генерации мнимых дуг (команды де-факто). Графовые пути возможностей утечки информации по графудоступа.

Тема 5. Модели безопасности на основе мандатной политики

Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа. Решетка уровней безопасности. Классы безопасных информационных потоков и матрица доступа.

Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы. Функция перехода системы из одного состояния в другое. Основная теорема безопасности (теорема безопасности Белла- ЛаПадулы). Недостатки и "абстрактность" систем на основе модели Белла-ЛаПадулы (Z-системы и др.).

Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы. Уполномоченные (доверенные) субъекты и авторизованная функция перехода МакЛина. Групповые субъекты доступа. Модель совместного доступа МакЛина. Правила безопасного доступа NRU и NWD для групповых субъектов.

Другие расширения модели Белла-ЛаПадулы. Модель Low-WaterMark.

Тема 6. Модели безопасности на основе тематической политики

Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа.

Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации. Тематическая решетка на корневом дереве рубрикатора при монорубрицированной иерархической классификации и ее изоморфный вариант в виде решетки листовых подмножеств.

Тематические мультирубрики при мультирубрицированной иерархической классификации субъектов и объектов доступа. Алгебра (решетка) мультирубрик. Отношения доминирования мультирубрик, операции (механизмы) наименьшей верхней и наибольшей нижней границ мультирубрик.

Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной тематической классификацией субъектов и объектов доступа.

Тема 7. Модели безопасности на основе ролевой политики

Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям. Сеансовый характер функционирования компьютерной системы с ролевым доступом. Сеансовая авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях).

Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.

Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др. Способы наделения правами доступа ролей (ролевых субъектов доступа) в системах с иерархической организацией ролей.

Модель индивидуально-группового доступа. Отличия рабочих групп от ролей. Теоретико- множественная формализация индивидуально-группового доступа.

MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

Тема 8. Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости

Понятие и общая характеристика скрытых каналов утечки информации. Скрытые каналы " по памяти", скрытые каналы " по времени", статистические скрытые каналы (" по

статистике"). Примеры реализации скрытых каналов утечки информации. Понятие емкости (пропускной способности) скрытых каналов передачиданных.

Автоматная модель информационного невлияния Гогена-Мессигера. Функция истории вводов и функция очищения. Модель Гогена-Мессигера как теоретико-методологическая база интерфейса защищенных КС в аспекте устранения (перекрытия) скрытых каналов утечки информации "по времени".

Теоретико-вероятностная трактовка информационного потока (по К.Шеннону). Модели информационной невыводимости и информационного невлияния как теоретико-методологическая основа анализа (выявления) и перекрытия скрытых каналов "по памяти" и "по статистике". Теоретико-вероятностная трактовка автоматной модели Гогена-Мессигера.

Технологии представлений (views) в реляционных СУБД как пример реализации подходов информационной невыводимости и информационного невлияния.

Тема 9. Модели и механизмы обеспечения целостности данных

Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостностиданных.

Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Объекты, требующие контроля целостности *(constrained data items),* процедуры проверки целостности *(integrity verification procedures),* корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект".

Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет " записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла- Лападулы).

Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадулы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись).

Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах. Принципы "атомарности" (неделимости), "изоляции" транзакций. Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей. Понятие и виды "грязных" (dirty) данных - "грязное чтение" (dirty read), "потерянные изменения"(lost update) и "неповторяющееся чтение" (unrepeatable read).

Протоколы выполнения и фиксации транзакций. Протоколы, основанные на "захватах" блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций). Тупики *(Deadlock),* их обнаружение и разрушение. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

1.1.1. Содержание практических занятий по дисциплине.

По разделу "Исходные положения теории компьютерной безопасности"

1. Методы анализа и методика экспертного оценивания угроз безопасности

По разделу "Модели безопасности компьютерных систем"

1. Решение задач по моделям безопасности на основе дискреционной политики
2. Решение задач по моделям безопасности на основе мандатной политики
3. Решение задач по моделям безопасности на основе тематической политики

По разделу "Методы анализа и оценки защищенности компьютерных систем"

1. Решение задач по теоретико-графовым моделям комплексной оценки защищенности
2. Решение задач по анализу и оптимизации систем индивидуально-группового назначения правдоступа

Тема: Модель Харрисона-Рузо-Ульмана (HRU)Задание № 1. Задача № 1.

Пусть имеется два субъекта: s_1 (доверенный пользователь, *admin)* и s_2 (обычный пользователь, *user).*

Пусть имеется два каталога (объекты) o_1 и o_2, владельцами которых являются пользователи s_1 и s_2, соответственно. В каталоге имеется объект o_3 с секретной информацией.

Права доступа в системе заданы исходным состоянием матрицы доступа:

	o_1- secret	o_2 - no secret	o_3 - secret
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*
s_2	**-**	***own,r,w,e***	**-**

Классический сценарий атаки с помощью троянской программы в системах, функционирующих на основе модели **HRU,** заключается в следующем.

1-й шаг. Субъект-злоумышленник s_2 создает в своем каталоге o_2 файл троянской программы $o_{тр}$, дает на него права *чтения r (read), записи w (write)* и *запуска e (execute)* для субъекта s_1, объявляет о каких-либо полезных свойствах и возможностях программы $o_{тр}$ и ожидает запуска доверенным пользователем s_1 троянской программы. Команда перехода и соответствующее изменение матрицы доступа выглядят следующим образом.

Command "создать файл" (s_2,$o_{тр}$,**):**

if *"write"* [s_2,o_2] then

Create object $o_{тр}$;

Enter {"own", "read","write","e xecute"}into [s_2, $o_{тр}$];

end if
if *{"read","write"}* ∈ [s_1 ,o_2] then

Enter
{ "read","write","exe
cute"} into [s_1, $o_{тр}$];
end if

end command

	o_1- secret	o_2 - no secret	o_3 – secret	o_4 - trojan
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*	*r,w,e*
s_2	-	*own,r,w,e*	-	*own,r,w,e*

2-й шаг. Доверенный субъект s_1 запускает троянскую программу $o_{тр}$, которая автоматически приобретаетего права доступа.

Command "запустить файл" (s_1,$o_{тр}$):

if *{"read","write","execute"}* ∈ [s_1,$o_{тр}$] then

Create subject $s_{тр}$;

Enter { "read","write","execute"} into [$s_{тр}$,o_2];

Enter
{ "read","write","execut
e"} into [$s_{тр}$,$o_{тр}$];end if

if *{"own",*
"read","write","execute
"} ∈ [s_1,o_1] and

{"own",
"read","write","execute
"} ∈ *[s_1,o_3]*

then
Enter {"read","write","execute"} into [$s_{тр}$,o_1];
Enter
{"read","write","exec
ute"} into [$s_{тр}$,o_3];
end if
end command

	o_1- secret	*o_2* - no secret	o_3 - secret	*o_{mp}*- trojan
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*	*r,w,e*
s_2	-	*own,r,w,e*	-	*own,r,w,e*
$s_{тр}$	*r,w,e*	*r,w,e*	*r,w,e*	*r,w,e*

3-й **шаг.** На основе скрытых (недекларируемых) возможностей троянская программа $s_{тр}$ копирует содержимое секретного файла o_3 в несекретный каталог o_2, обеспечивая возможность недоверенному пользователю ознакомиться с секретной информацией, прямо ему недоступной.

Command "скопировать файл o_3 программой s_{mp} в o_2" ($s_{тр}$,o_3,o_2):

if *"read"* $\in$ [$s_{тр}$,o_3] and *"write"* $\in$ [$s_{тр}$,o_2] then

Create object o';

Enter {"own", "read","write","execute"} into [$s_{тр}$,o'];

Enter "read" into [s_2,o']; Read ($s_{тр}$,o_3);

Write (s_{mp},o');

end if
Destroy subject s_{mp};

end command

	o_1- secret	o_2 - no secret	o_3 - secret	o_{mp}- trojan	$o' \subset o_3$ - secret
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*	*r,w,e*	-
s_2	-	*own,r,w,e*	-	*own,r,w,e*	*r*

Задание. Построить сценарий аналогичной атаки в том случае, когда доверенный пользователь s_1 в исходном состоянии имеет на каталог o_2 только права *чтения r.* Отобразите соответствующие последовательности команд перехода и изменений матрицы доступа.

Исходное состояние матрицы доступа.

	o_1 - secret	o_2 - no secret	o_3 - secret
s_1	*own,r,w,e*	*r*	*own,r,w,e*
s_2	-	*own,r,w,e*	-

Решение.

Возможны два варианта.

1- й вариант.

1-й шаг. Пользователь-злоумышленник $\boldsymbol{s}_2$, являясь владельцем каталога $\boldsymbol{o}_2$, дает на него недостающие права доверенному пользователю $\boldsymbol{s}_1$.

Command "дать права на каталог от владельца"
($\boldsymbol{s}_1$,$\boldsymbol{s}_2$,$\boldsymbol{o}_2$)**:**if *"own"* $\in$ [$\boldsymbol{s}_2$,$\boldsymbol{o}_2$]

then
Enter *{"write","execute"}* ***into***
[$\boldsymbol{s}_1$,$\boldsymbol{o}_2$]**;**end if

end command

	o_1 - secret	o_2 - no secret	o_3 - secret
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*
s_2	-	*own,r,w,e*	-

Последующие шаги аналогичны, описанным выше.

2- й вариант.

1-й шаг. Если по каким-либо соображениям пользователь-злоумышленник $\boldsymbol{s}_2$, не может давать доверенному пользователю права *записи* ***w*** и *запуска* ***e*** на каталог $\boldsymbol{o}_2$, то под каким-либо

обоснованным предлогом он создает новый каталог o_4, и, являясь его владельцем, дает на него доверенному пользователю s_1 права *чтения* ***r***, *записи* ***w*** и *запуска* ***e***.

Command "создать каталог" (s_2, o_4)**:*Create object o*4;**

Enter {*"own", "read","write","execute"*} ***into*** [s_2,o_4]**;**

Enter {*"read","write","execute"*} ***into*** [s_1,o_4]**;end command**

	o_1 - secret	o_2 - no secret	o_3 – secret	o_4-no secret
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*	*r,w,e*
s_2	-	*own,r,w,e*	-	*own,r,w,e*

В дальнейшем файл троянской программы $o_{тр}$ создается в каталоге o_4 и последующие шаги аналогичны, описанным выше.

Тема: Модели ТАМ

Задание № 1.

Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа, имеется тритипа сущностей (субъектов и объектов доступа) – ***u***, ω и ν .

Пусть в начальном состоянии системы имеется субъект s_1 типа ***u*** - (s_1: ***u***).

Осуществляется переход системы в новое состояние посредством следующей команды: α(s_1:***u***, s_2:ω, o_1:ν):

Create object o_1 ***of type*** ν **;**

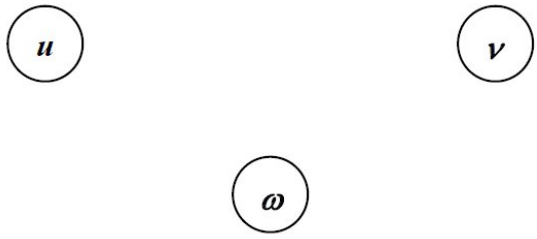
Inter r into [s_1, o_1] **;**

Create subject s_2 ***of type*** ω **;**

Inter r′ into [s_2, o_1] **;**

Create subject s_3 ***of type u*** **;**

Inter r″ into [s_3, o_1] **;end** α

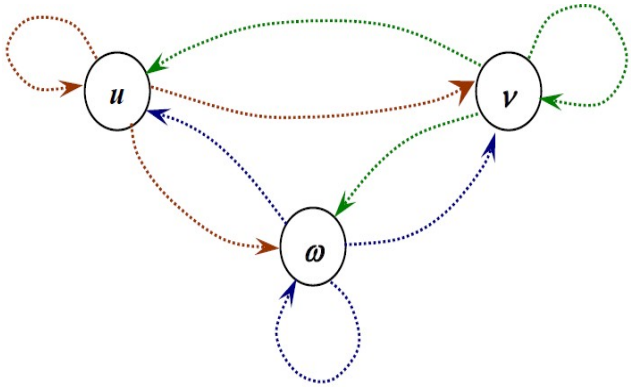


при выполнении которой создается объект типа ν, на него устанавливаются права ***r*** для субъекта s_1, инициализируются дополнительные субъекты - s_2 типа ω и s_3 типа ***u***, им права ***r′*** и на ***r″*** объект o_1, соответственно.

Задание. Построить по команде α граф отношений наследственности.

Решение.

В команде α три дочерних типа ν, ω и ***u*** по отношению к типам, задействованным в теле команды - ***u***, ω, ν .



Поэтому в графе отношений наследственности возникают следующие дуги – (***u***,ν), (***u***,ω), (***u***,***u***), (ω,ν), (ω,ω),(ω,***u***), (ν,ν), (ν,ω), (ν,***u***).

Следует обратить внимание на то, что на Графе отношений наследственности в результате выполнения команды перехода α возникло несколько циклов длиной 2 и более– (***u***→ω→ν→ ***u***), (***u***→ω→***u***), (ω→***v***→ω), (***u***→***v***→***u***).

Задание 2.

Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа **ТАМ**, имеетсядва субъекта доступа: субъект s_1 типа ***a*** - (***s***$_1$: ***a***) доверенного пользователя (*admin*); субъект s_2 типа ***u*** - (***s***$_2$: ***u***) обычного пользователя (*user*); а также три объекта доступа: каталог o_1 типа ν (*secret*) – (***o***$_1$: ν), владельцем которого является пользователь s_1 (*"own"*∈ r_{s1},o_1), несекретный каталог o_2 типа η (*no secret*) – (***o***$_2$: η), владельцем которого является пользователь s_2 (*"own"*∈ r_{s2},o_2), секретный файл o_3 типа ν – (***o***$_3$: ν) в каталоге o_1, владельцем которого также является пользователь s_1 (*"own"*∈ r_{s1},o_3).

Пользователь s_1 имеет также права *чтения*, *записи* и *запуска* на объект o_2

r_{s1},o_2) ({*"read","write","execute"*} ⊆

.

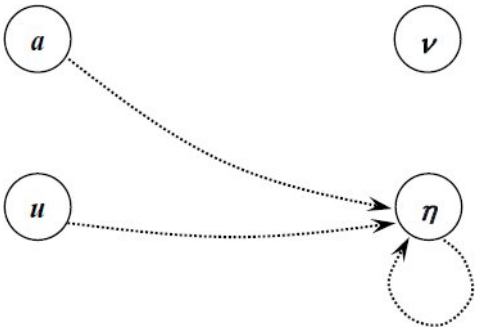
В исходном состоянии Графа наследственности имеется четыре вершины.

Задание. Построить Граф отношений наследственности по сценарию атаки троянским конем со стороны

пользователя s_2 на секретный файл
o_3.

Решение.

1- й шаг. Субъект-злоумышленник s_2 создает в своем каталоге o_2 файл троянской программы $o_{тр}$ типа η, дает на него права *чтения* ***r***, *записи* ***w*** и *запуска* ***e*** (*execute*) для субъекта s_1, объявляет о каких-либо полезных свойствах и возможностях программы $o_{тр}$ и ожидает запуска доверенным пользователем s_1 троянской программы. Команда перехода в нотации модели **ТАМ** выглядит следующим образом.



$\alpha_1(s_1{:}a, s_2{:}u, o_2{:}\eta, o_{тр}{:}\eta)$:

if *"write"* ∈ r_{s2}, o_2 then ***Create object*** $o_{тр}$ ***of type*** η;

Enter {*"own", "read","write","execute"*}

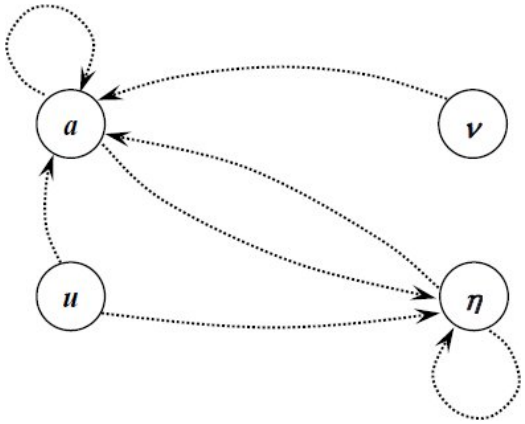
into r_{s2}, $o_{тр}$;
end if

if {*"read","write"*} ⊆ r_{s1},o_2 then ***Enter*** {*"read","write","execute"*} ***into*** r_{s1}, $o_{тр}$;**end if**

end α_1

В команде α_1 дочерним типом является тип η по отношению к типам ***a***, ***u*** и η, входящим в тело команды. Поэтому в результате перехода системы в новое состояние по команде α_1 в Графе отношений наследственности появляются следующие дуги – **(*a*,η), (*u*,η) и (η,η).**

2- й шаг. Доверенный субъект s_1 запускает троянскую программу $o_{тр}$, которая автоматически приобретает его права доступа.



Command "запустить файл"
(s_1,$o_{тр}$)**:** $\alpha_2(s_1{:}a, s_{тр}{:}\eta, o_1{:}\nu, o_2{:}\eta,$
$o_3{:}\nu, o_{тр}{:}\eta)$:

if {*"read","write","execute"*} ⊆ r_{s1}, $o_{тр}$ then

Create subject $s_{тр}$ ***of type a*;**

Enter {*"read","write","execute"*} ***into*** $r_{\text{стр}}$, o_2;

end if
if {*"own", "read","write","execute"*} ⊆ r_{s1},o_1 and {*"own", "read","write","execute"*} ⊆ r_{s1}, o_3 then

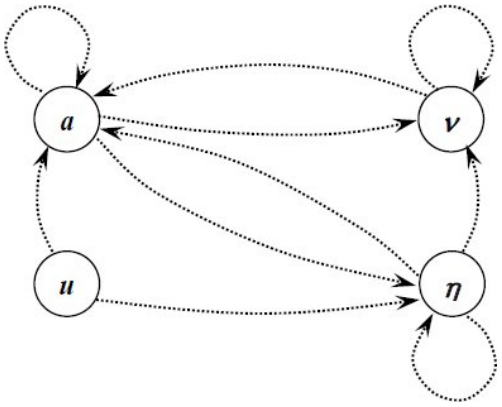
Enter {*"read","write","execute"*} ***into*** $r_{\text{стр}}$, o_1; ***Enter*** {*"read","write","execute"*} ***into*** $r_{\text{стр}}$, o_3;
end if

end α_2

В команде α_2 дочерним типом является тип ***a*** по отношению к типам ***a***, **η**, ***u*** и **ν**, входящим в тело команды. Поэтому в результате перехода системы в новое состояние по команде α_2 в Графе отношений наследственности появляются следующие дуги – (***a***,***a***), (**η**,***a***), (***u***,***a***) и (**ν**,***a***).

Следует заметить, что уже на данном шаге в Графе отношений наследственности появляется цикл длиною два - (***a***→**η**), отражающий угрозу переноса в объекты несекретного типа **η** информации от доверенного пользователя s_1.

3- й шаг. На основе скрытых (недекларируемых) возможностей троянская программа $s_{\text{тр}}$ типа ***a*** копирует содержимое секретного файла o_3 типа **ν** в несекретный каталог o_2 типа **η**, обеспечивая возможность недоверенному пользователю s_2 типа ***u*** ознакомится с секретной информацией типа **ν**,



прямо ему недоступной.

α**3**($s_{\text{тр}}$:***a***, o_3:ν, o_2:η, ***o'***:ν):

if *"read"* ∈ $r_{\text{стр}}$,o_3 and *"write"* ∈ $r_{\text{стр}}$, o_2 then ***Create object o' of type*** ν **;**

Enter {*"own", "read","write","execute"*} ***into*** $r_{\text{стр}}$, ***o'*** **;**

Enter *"read"* ***into*** r_{s2},o_1**;**

Read ($s_{\text{тр}}$ ***of type a***, o_3 ***of type*** ν)**;** ***Write*** ($s_{\text{тр}}$ ***of type a***, ***o' of type*** ν)**;** end if

Destroy subject $s_{\text{тр}}$ ***of type a*****; end** α_3

В команде α_3 дочерним типом является тип **ν** по отношению к типам ***a***, **η**, и **ν**, входящим в тело команды. Поэтому в результате перехода системы в новое состояние по команде α_3 в Графе отношений наследственности появляются следующие дуги – **(*a*,ν), (η,ν) и (ν,ν).**

На графе отношений наследственности появляется еще два цикла, длиной 2 - **(*a*→ν→ *a*)**, и диной 3 -
(*a*→η→ν→ *a*).

Задание 3.

В системе, функционирующей на основе модели с типизованной матрицей доступа **ТАМ** и

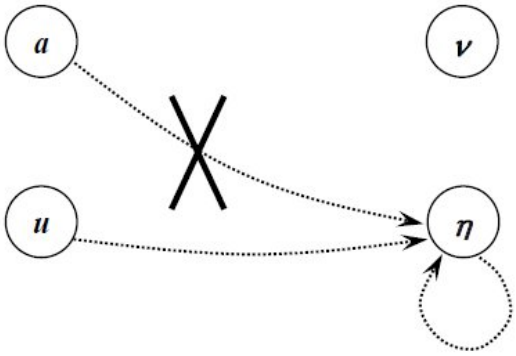
по условиям задачи 2.2, предложить возможное разрешение проблемы атак троянским конем на основе ограничений на команды переходов по соотношению дочерних и родительских типов. Дайте физическое обоснование решения и подтвердите его на Графе отношений наследственности.

Решение.

Возможны два варианта.

1-й вариант.

Вводится запрет на команды переходов $\alpha_{a\eta}$ в которых тип **η** (*no secret*) является дочерним для типа ***a***
(*admin*).



Это означает, что если при переходе в новое состояние создается объект типа **η**, то в команде перехода $\alpha_{a\eta}$ не могут быть задействованы субъекты типа ***a***. Тем самым злоумышленник не может, создавая несекретный объект типа **η**, одновременно давать на него права доступа доверенному пользователю типа ***a***.

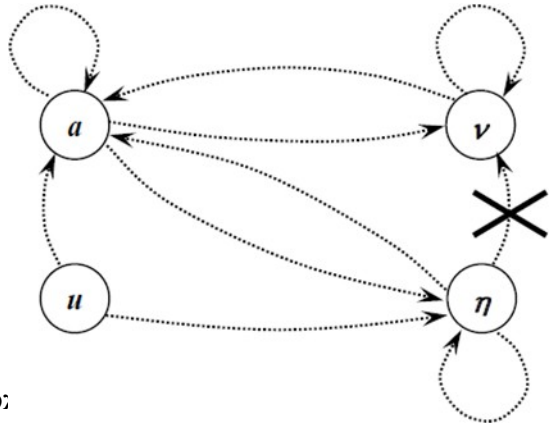
Таким образом, вторая часть команды α_1 невозможна.

На Графе отношении наследственности такие ограничения на первом шаге приведут к редукции дуги(***a***,**η**), что, в свою очередь устраняет возможность образования цикла (***a***→**ν**→ ***a***).

2-й вариант.

Вводится запрет на команды переходов $\alpha_{\eta\nu}$ в которых тип **ν** является дочерним для типа .

Это означает, что если при переходе в новое состояние создается секретный объект типа **ν**, то при этом в команде перехода $\alpha_{\eta\nu}$ не могут быть задействованы несекретные сущности типа **η**. Тем самым создание секретного файла типа **ν** в несекретном каталоге типа **η** невозможно.



Таким образом, команда α_3 невозмо:

На Графе отношений наследственности такие ограничения приводят к редукции дуги **(η,ν),** что, в своюочередь устраняет возможность образования **цикла (*a*→η→ν→ *a*).**

***Тема*. Модели TAKE-GRANT**

Задача № 3.1

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов ***Г***0 (***O, S, E***), в которой сущности ***x*** и ***y*** связаны ***tg***-путем.

Задание: построить систему команд перехода передачи субъекту ***x*** прав доступа α на объект ***s*** от субъекта ***y***.

Решение 1-й шаг. Субъект ***s***2 на основе своего права ***t*** ("брать") на субъект ***y*** берет у него право α на объект ***s***

– ├***takes***(α, ***s***2, ***y***, ***s***).

Преобразование Графа доступов ***Г***0 (***O, S, E***) в новый Граф ***Г***1 (***O, S, E***) доступов выглядит следующим образом

2-й шаг. Субъект ***s***2 предоставляет на основе права ***g*** ("давать") субъекту ***s***1свое право α на объект - ***s***

–

├***grants***(α, ***s***2, ***s***1, ***s***).

Преобразование Графа доступов ***Г***1 (***O, S, E***) в новый Граф ***Г***2 (***O, S, E***) доступов выглядит следующим образом **3-й шаг.** Субъект ***x*** берет на основе своего права ***t*** ("брать") на субъект ***s***1 имеющееся у него право α на объект ***s*** – ├***takes***(α, ***x***, ***s***1, ***s***).

Преобразование Графа доступов ***Г***2 (***O, S, E***) в новый Граф ***Г***3 (***O, S, E***) доступов выглядит следующим образом В итоге субъект ***x*** через ***tg***-путь получает у субъекта ***y*** права доступа α на объект ***s***.

α ⊗ ***t g t x y s s***1 ***s***2 ***Г***0 (***O, S, E***) α ⊗ ***t g t x y s s***1 ***s***2 ***Г***1 (***O, S, E***) α α ⊗ ***t g t x y s s***1 ***s***2 ***Г***2 (***O, S, E***) α α α ⊗ ***t g***

t x y s s1 ***s***2 ***Г***3 (***O, S, E***) α α α 197

Задача № 3.2 Для иллюстрации возможности передачи прав доступа по ***tg***-пути независимо от направления прав ***t*** и ***g***, изменяются в условиях задачи 3.1 направление права между субъектами ***s***1 и ***s***2.

Задание: построить систему команд перехода передачи субъекту ***x*** прав доступа α на объект ***s*** от субъекта ***y***. **Решение 1-й шаг.** Аналогичен в решении задачи 3.1 (субъект ***s***2 на основе своего права ***t*** ("брать") на субъект ***y*** берет у него право α на объект ***s*** – ├***takes***(α, ***s***2, ***y, s***).

Преобразование Графа доступов ***Г***0 (***O, S, E***) в новый Граф ***Г***1 (***O, S, E***) доступов выглядит следующим образом **2-й шаг.** Субъект ***s***1 создает субъект ***z*** с правами на него ***tg*** и предоставляет на него право ***g*** ("давать") субъекту ***s***2 – Преобразование Графа доступов ***Г***1 (***O, S, E***) в новый Граф ***Г***2 (***O, S, E***) доступов выглядит следующим образом **3-й шаг.** Субъект ***s***2 предоставляет имеющееся у него право α на объект ***s*** субъекту ***z***, а субъект ***s***1, используя свое право ***t*** на субъект ***z*** берет у него право α на объект ***s*** – Преобразование Графа доступов ***Г***2 (***O, S, E***) в новый Граф ***Г***3 (***O, S, E***) доступов выглядит следующим образом **4-й шаг.** Аналогичен 3-му шагу в решении задачи 3.1.

α ⊗ ***t g t x y s s***1 ***s***2 ***Г***0 (***O, S, E***) α ⊗ ***t g t x y s s***1 ***s***2 ***Г***1 (***O, S, E***) α ├***create***(***tg***, ***s***1, ***z***) ***grants***(***g***, ***s***1, ***s***2, ***z***) ***z*** α ⊗ ***t g t x y s s***1 ***s***2 ***Г***2 (***O, S, E***) α ***tg g*** ├ ***grants***(α, ***s***2,***z, s***) ***takes***(***g***, ***s***1, ***s***2, ***z***) ***z*** α ⊗ ***t g t x y s s***1 ***s***2 ***Г***3 (***O, S, E***) α ***tg g*** αα 198 **Задача № 3.3**. Похищение прав доступа Пусть имеется система субъектов и объектов доступа, представленная Графом доступов ***Г***0 (***O, S, E***).

Установленная для системы политика безопасности запрещает любым субъектам (владельцам) предоставлять право α на "свои" объекты другим субъектам (но не запрещает субъектам, которые владеют правами ***t*** ("брать") на какие-либо субъекты брать у них права на их объекты).

Кроме субъекта ***s***, субъект ***u*** может быть связан ***tg***-путем с другими субъектами.

Задание: построить систему команд получения субъектом ***s*** прав доступа α на объект ***w*** от субъекта ***u***, при условии того, что команда ***grants***(α, ***u, s, w***) не может быть задействована.

Решение 1-й шаг. Пусть найдется субъект ***v***, имеющий право ***t*** на объект ***u***. При этом субъект ***u*** также имеет право ***t*** на субъект ***v***.

2- й шаг. Субъект ***u*** предоставляет субъекту ***s*** право ***t*** на субъект ***v*** – ├***grants***(***t***, ***u, s, v***).

3- й шаг. Субъект ***s*** берет у субъекта ***v*** право ***t*** на субъект ***u*** – ├***takes***(***t***, ***s, v, u***).

4- й шаг. Субъект ***s*** берет (похищает) у субъекта ***u*** право α на объект ***w*** – ├***takes***(α, ***s,*** α ***g w s u Г***0 (***O, S, E***) ***grants***(α, ***u, s, w***) ⊗ α ***g w s u Г***1 (***O, S, E***) ⊗ ***t t v*** α ***g w s u Г***2 (***O, S, E***) ⊗ ***t t t v*** α ***g w s u Г***3 (***O, S, E***) ⊗ ***t t t v t***α ***g w s u Г***4 (***O, S, E***) ⊗ ***t t t v t*** 199 ***u, w***).

Расширенная модель TAKE-GRANTЗадание 1.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов ***Г***0 (***O, S, E***), Пусть неявные каналы чтения, генерируемые различными командами "де-факто" имеют следующую стоимость: - ***r*spy** = 1, ***r*post** = 2, ***r*find** = 3 и ***r*pass** = 4.

Задание: Применяя команды "де-факто" сгенерировать все возможные неявные каналы чтения субъектом ***x***
информации из субъекта ***y***, и сравнить их стоимость.

Решение 1-й вариант 1-й шаг. ├***spy***(***x***, ***s***1, ***s***2).

2-й шаг. ├***spy***(***x***, ***s***2, ***s***y).

Общая стоимость затрат на реализацию неявного канала по первому варианту 1 + 1 = 2.
2-й вариант 1-й шаг. ***├post(x, s1, s2).***

2-й шаг. ***├spy(x, s2, sy).***

Общая стоимость затрат на реализацию неявного канала по второму варианту 2 + 1 = 3.
α ***Г0 (O, S, E) r r r x s1 s2 y w Г1 (O, S, E) r r r x s1 s2 y w r*** (=1) ***Г2 (O, S, E) r r r x s1 s2 y w r*** (=1) ***r*** (=1) ***Г1 (O, S,E) r r r x s1 s2 y w r*** (=2) ***r r r x s1 s2 y w r*** (=2) ***r*** (=1) 200 **3-й вариант 1-й шаг.** ***├pass(s1, s2, y).***

2-й шаг. ***├spy(x, s1, y).***

Общая стоимость затрат на реализацию неявного канала по третьему варианту 4 + 1 = 5.
Г1 (O, S, E) r r r x s1 s2 y w r (=4) ***Г1 (O, S, E) r r r x s1 s2 y w r*** (=1) ***r*** (=4) 201

Тема: Модели Белла-ЛаПадуллы

Пусть имеется мандатная система доступа **Σ(v_0,*Q*, F_T)**, в которой решетка уровней безопасности Λ**L**

является линейной и имеет три уровня – l_1, l_2, l_3; $l_1 > l_2 > l_3$; $l_1 > l_3$.

Пусть имеется следующая система субъектов (пользователей) доступа:
u_1 – администратор системы; u_2 – руководитель предприятия; u_3 – делопроизводитель;
u_4 – user, т.е. рядовой непривилегированный пользователь.Пусть имеется следующая система объектов доступа:
o_1 – системное ПО;

o_2 – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";
o_3 – документ "Приказ о поощрении работников по случаю Дня Предприятия";
$o4$ – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).

Задание 2.

Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступаи матрицу доступа ***A*[*u,o*]** .

Решение 1. Начинать необходимо с установки уровней безопасности объектов доступа, чтобы на этойоснове с учетом правил ***NRU*** и ***NWD*** определить уровни допуска субъектов доступа.

Очевидно, что наиболее конфиденциальная информация содержится в объекте o_2. Таким образом $f_L(o_2) = l_1$.

Также очевидно, что в системном ПО каких-либо секретов предприятия (кроме самого факта использования конкретного ПО) не содержится. Таким образом $f_L(o_1) = l_3$.

Объект o_3 коммерческих, производственных и др. секретов также не содержит, кроме персональных данных работников предприятия, и по своей сути поэтому должен быть доступен всем работникам предприятия. Поэтому $f_L(o_3) = l_3$.

АИС "Борей" содержит коммерческие секреты предприятия, но, конечно же, в отличие от объекта o_2, не самого высокого уровня. Поэтому $f_L(o_4) = l_2$.

2. Основываясь на анализе функций и полномочий пользователей, с учетом правил ***NRU*** и ***NWD*** устанавливаем уровни допуска субъектов доступа.

Поскольку функции и полномочия администратора системы заключаются, прежде всего, в

установке и сопровождении ПО, то он должен иметь возможность вносить при необходимости изменения в ПО. Учитывая правило ***NWD***, получаем $f_L(u_1)= l_3$.

Наивысшие полномочия у руководителя предприятия, поэтому $f_L(u_2)=l_1$.

Делопроизводитель должен иметь возможность готовить конфиденциальные документы (уровней l_1 и l_2). Учитывая правило *NWD*, получаем $f_L(u_3)= l_2$.

У непривилегированного пользователя соответственно наименьшие полномочия, поэтому $f_L(u_4)= l_3$.

3. Непосредственное применение правил ***NRU*** и ***NWD*** дает следующую матрицу доступа

$A'[u,o]$	$o1$	$o2$	$o3$	$o4$	
=	*r,w*	w	r,w	w	$u1$
	r	r,w	r	r	$u2$
	r	w	r	r,w	$u3$
	r	w	r,w	w	$u4$

4. Очевидно, что права некоторых пользователей по правилам ***NRU*** и ***NWD*** (матрица $A'[u,o]$) являются избыточными.

Так, для пользователя u_1 (администратор) и для пользователя u_4 не являются необходимыми иоправданными права записи в объекты o_2, o_3 и o_4.

Для пользователя u_3 (делопроизводитель) не нужны права записи в объект o_2 (после того, как документ утвержден и введен в действие).

Таким образом получаем матрицу доступа, "уточняющую" и корректирующую права доступа, получаемые пользователями по правилам ***NRU*** и ***NWD***.

$A[u,o]$	$o1$	$o2$	$o3$	$o4$	
=	*r,w*	-	r	-	$u1$
	r	r,w	r	r	$u2$
	r	-	r	r,w	$u3$
	r	-	r	-	$u4$

Задача № 5.2.

Составить и обосновать систему допусков и грифов секретности для двух состояний системы:

Состояние I – Подготовка (разработка) документа o_2.

Состояние II – Документ o_2 утвержден и введен в действие.

Является ли переход системы из **состояния I** в **состояние II** безопасным по МакЛину?

Решение

1. Состояние II описано в результатах решения задачи 5.1.
2. Документ готовится по заданию руководителя (пользователь u_2) делопроизводителем (пользователь u_3). Поскольку уже на этапе подготовки он может содержать наиболее конфиденциальные сведения, то $f_L(o_2)= l_1$. Тогда для того, чтобы пользователь u_3 мог вносить в него данные, по правилам ***NRU*** и ***NWD*** необходимо $f_L(u_3)=l_1$.

Однако уровень допуска $f_L(u_3)=l1$ по правилам ***NRU*** и ***NWD*** автоматически приведет к невозможности (запрету) для делопроизводителя (пользователь u_3) исполнять документы по заказам клиентов (запись в объект o_4). В результате для обеспечения непрерывности делового цикла в **состоянии I** необходимо также .

$f_L(o_4)= l_1$.

Матрица доступа в **состоянии I** выглядит следующим образом:

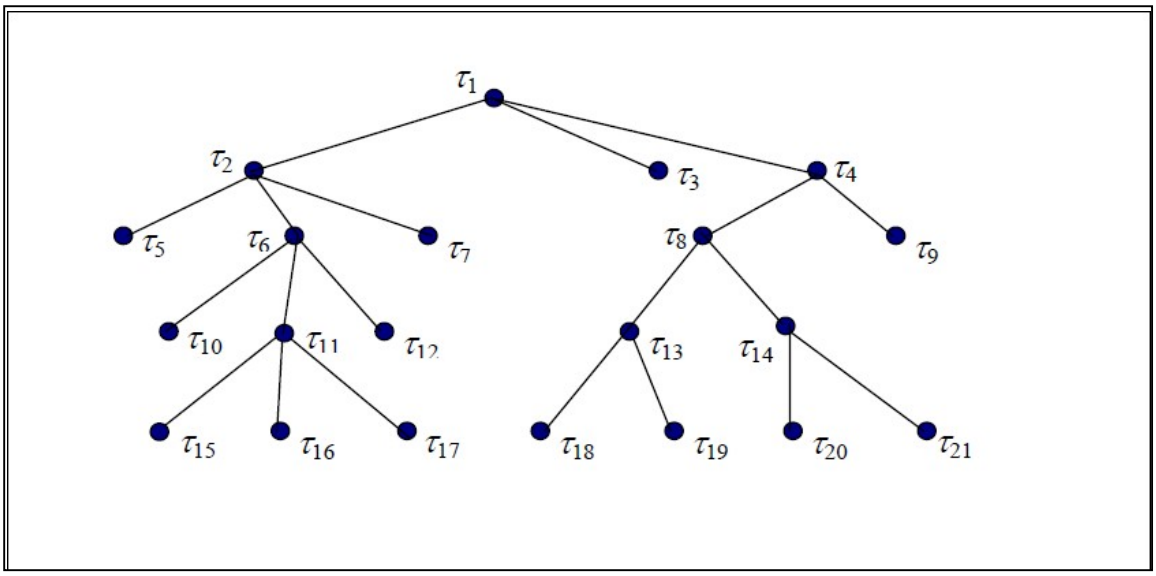
$o1$	$o2$	$o3$	$o4$	
r,w	-	r	-	$u1$

$A[u,o]$ =					
r	r,w		r	u_2
r	- r,w	r	r,wr	u_3
r	-	r	-	u_4

Поскольку при переходе из состояния I в состояние II изменяются сразу два аспекта безопасности – одновременно снижается уровень допуска пользователя u_3 и гриф секретности объекта o_4, – то по условиям Теоремы безопасности МакЛина такой переход небезопасен. В частности в состоянии I пользователь одновременно работая по правам ***r,w*** с объектами o_2, o_4 может перенести конфиденциальную информацию из объекта o_2 в объект o_4, который при переходе в состояние II станет доступным по чтению пользователям с уровнем допуска l_2, и тем самым создадутся условия информационного потока "сверху-вниз".

Тема: Модели тематического разграничения доступа на основе иерархических рубрикаторов

Пусть имеется иерархический тематический рубрикатор. Для тематической классификации сущностейсистемы (субъектов и объектов доступа) использованы мультирубрики:



$Ť^{M}_{1}$={$_{5}$, $_{6}$}; $Ť^{M}_{2}$={$_{11}$, $_{12}$}; $Ť^{M}_{3}$={$_{3}$, $_{8}$}; $Ť^{M}_{4}$={$_{6}$, $_{8}$};
$Ť^{M}_{5}$={$_{12}$, $_{13}$};$Ť^{M}_{6}$={$_{13}$, $_{9}$}; $Ť^{M}_{7}$={$_{15}$, $_{16}$, $_{14}$};

Задача № 6.1.

Определить отношения доминирования (уже, шире, несравнимо) между следующими мультирубриками:
$Ť^{M}_{2}$ и $Ť^{M}_{1}$; $Ť^{M}_{7}$ и $Ť^{M}_{4}$; $Ť^{M}_{5}$ и $Ť^{M}_{3}$; $Ť^{M}_{6}$ и $Ť^{M}_{4}$

Решение.
$Ť^{M}_{2} \leq Ť^{M}_{1}$; $Ť^{M}_{7} \leq Ť^{M}_{4}$; $Ť^{M}_{5} <> Ť^{M}_{3}$; $Ť^{M}_{6} <> Ť^{M}_{4}$

Задача № 6.2.

Построить объединение следующих мультирубрик:

$Ť^{M}_{3} \cup Ť^{M}_{5}$; $Ť^{M}_{4} \cup Ť^{M}_{6}$; $Ť^{M}_{2} \cup Ť^{M}_{3}$; $Ť^{M}_{1} \cup Ť^{M}_{2}$; $Ť^{M}_{4} \cup Ť^{M}_{7}$

Решение

$Ť^{M}_{3} \cup Ť^{M}_{5}$

1. Шаг. Производим теоретико-множественное объединение наборов рубрик соответствующих мультирубрик. Получаем первый промежуточный объединенный набор {$_{3}$, $_{8}$, $_{12}$,$_{13}$}

В объединенном наборе рубрика $_{13}$ доминируется (ниже по иерархии) рубрикой $_{8}$ и поэтому исключается из объединенного набора - {$_{3}$, $_{8}$, $_{12}$};

2. Шаг. Проверяем второй промежуточный набор - {$_{3}$, $_{8}$, $_{12}$}, на предмет наличия полного набора сыновей какой–либо рубрики. Таковых нет.

3. Результат - $Ť^{M}_{3} \cup Ť^{M}_{5}$={$_{3}$, $_{8}$, $_{12}$}. Следует обратить внимание, что результат объединения мультирубрик сам является мультирубрикой, т.е. в нем нет подчиненных рубрик и полного набора сыновей какой- либо рубрики.

$Ť^{M}_{4} \cup Ť^{M}_{6}$

1. Шаг. {$_{6}$, $_{8}$, $_{13}$,$_{9}$}. $_{13}$ доминируется $_{8}$. {$_{6}$, $_{8}$, $_{9}$}.

2.Шаг. Рубрики $_{8}$, $_{9}$ является полным набором сыновей рубрики $_{4}$. Поэтому во втором промежуточномнаборе вместо рубрик $_{8}$, $_{9}$ ставим {$_{4}$, $_{6}$}.

3.Результат - $Ť^{M}_{4} \cup Ť^{M}_{6}$={$_{4}$, $_{6}$}.

$Ť^{M}_{2} \cup Ť^{M}_{3}$

1. Шаг. {$_{11}$, $_{12}$, $_{3}$,$_{8}$}. Домируемых рубрик нет. **2.Шаг.** {$_{11}$, $_{12}$, $_{3}$,$_{8}$}. Полных наборов сыновей нет.**3.Результат** - **$Ť^{M}_{2} \cup Ť^{M}_{3}$**={$_{11}$, $_{12}$, $_{3}$,$_{8}$}

$Ť^{M}_{1} \cup Ť^{M}_{2}$

1.Шаг. {$_{5}$, $_{6}$, $_{11}$,$_{12}$}. $_{11}$,$_{12}$ доминируются $_{6}$. {$_{5}$, $_{6}$}.

2. Шаг. {$_{5}$, $_{6}$}. Полных наборов сыновей нет.

3. Результат - $Ť^{M}_{1} \cup Ť^{M}_{2}${$_{5}$, $_{6}$}= $Ť^{M}_{1}$. Следует обратить внимание, что объединенная мультирубрика всегдадоминирует над объединяемыми и является их наименьшей верхней границей.

$Ť^{M}_{4} \cup Ť^{M}_{7}$

1.Шаг. {$_{6}$, $_{8}$, $_{15}$,$_{16}$, $_{14}$}. $_{14}$ доминируются $_{8}$. $_{15}$, $_{16}$ доминируются $_{6}$. {$_{6}$, $_{8}$}.

2. **Шаг.** {▶6, ▶8}. Полных наборов сыновей нет.
3. **Результат -** $\check{T}^{M_4} \cup \check{T}^{M_7}\{▶6, ▶8\} = \check{T}^{M_4}$.

Задача № 6.3.

Построить пересечение следующих мультирубрик:

$\check{T}^{M_3} \cap \check{T}^{M_5}$; $\check{T}^{M_4} \cap \check{T}^{M_6}$; $\check{T}^{M_2} \cap \check{T}^{M_3}$; $\check{T}^{M_1} \cap \check{T}^{M_2}$; $\check{T}^{M_4} \cap \check{T}^{M_7}$

Решени

е. $\check{T}^{M_3} \cap \check{T}^{M_5}$

1. **Шаг.** {▶3, ▶8}↔{▶12, ▶13}. В наборе мультирубрики $\check{T}^{M_3}$={▶3, ▶8} оставляем те рубрики, которые доминируются (ниже по иерархии) какими-либо рубриками мультрубрики $\check{T}^{M_5}$={▶12, ▶13}.Таковых нет. Таким образом, первый набор - ∅.
2. **Шаг.** {▶3, ▶8}↔{▶12, ▶13}. В наборе мультирубрики $\check{T}^{M_5}$={▶12, ▶13} оставляем те рубрики которые

доминируются (ниже по иерархии) какими-либо рубриками мультрубрики $\check{T}^{M_3}$={▶3, ▶8}. Таковой рубрикой является

▶13 (доминируется рубрикой ▶8). Таким образом, второй набор - {▶13 }.

3. **Шаг.** Производим теоретико-множественное объединение первого и второга набора.

Результат - $\check{T}^{M_3} \cap \check{T}^{M_5}$={▶13 }.

$\check{T}^{M_4} \cap \check{T}^{M_6}$

1.Шаг. {▶6, ▶8}↔{▶13, ▶9}. От набора первой мультирубрики - ∅. **2.Шаг.** {▶6, ▶8}↔{▶13, ▶9}. От набора второй мультирубрики - {▶13}.**3.Шаг.** Результат - $\check{T}^{M_4} \cap \check{T}^{M_6}$={▶13}.

$\check{T}^{M_2} \cap \check{T}^{M_3}$

1.Шаг. {▶11, ▶12}↔{▶3, ▶8}. От набора первой мультирубрики - ∅. **2.Шаг.** {▶11, ▶12}↔{▶3, ▶8}. От набора второй мультирубрики - ∅. **3.Шаг.** Результат - $\check{T}^{M_2} \cap \check{T}^{M_3}$= ∅.

$\check{T}^{M_1} \cap \check{T}^{M_2}$

1. **Шаг.** {▶5, ▶6}↔{▶11, ▶12}. От набора первой мультирубрики - ∅.
2. **Шаг.** {▶5, ▶6}↔{▶11, ▶12}. От набора второй мультирубрики - {▶11, ▶12}.
3. **Шаг.** Результат - $\check{T}^{M_1} \cap \check{T}^{M_2}$={▶11, ▶12}. Следует обратить внимание, что пересечение мультирубрикявляется мультирубрикой и их набольшей нижней границей.

$\check{T}^{M_4} \cap \check{T}^{M_7}$

1.Шаг. {▶6, ▶8}↔{▶15, ▶16, ▶14}. От набора первой мультирубрики - ∅.

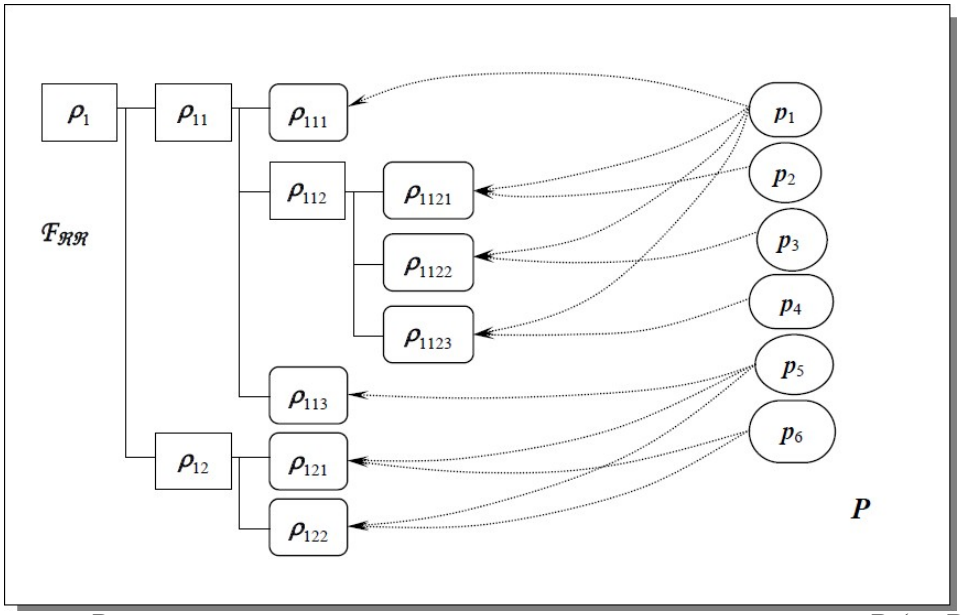
2.Шаг. {▶6, ▶8}↔{▶15, ▶16, ▶14}. От набора второй мультирубрики - {▶15, ▶16, ▶14}.

3.Шаг. Результат - $\check{T}^{M_4} \cap \check{T}^{M_7}$={▶15, ▶16, ▶14}.

Тема: Модели ролевого доступа при иерархически организованной системе ролей

Задача № 7.1.

Пусть имеется система иерархически организованных ролей $\Re$ **(ρ∈$\Re$),** представленная на рис.



Ролям назначены полномочия из конечного множества ***P*** (***p*∈*P***).

Определить тип наделения ролей полномочиями (листовой таксономический, листовойнетаксономический, иерархически охватный).

Определить полномочия роли ρ_{11}.

Решение.

Ввиду того, что полномочия непосредственно назначаются только листовым ролям, то имеем листовойподход.

Так как, одно и то же полномочие, например p_1, назначается сразу нескольким ролям, то имеемнетаксономический листовой подход.

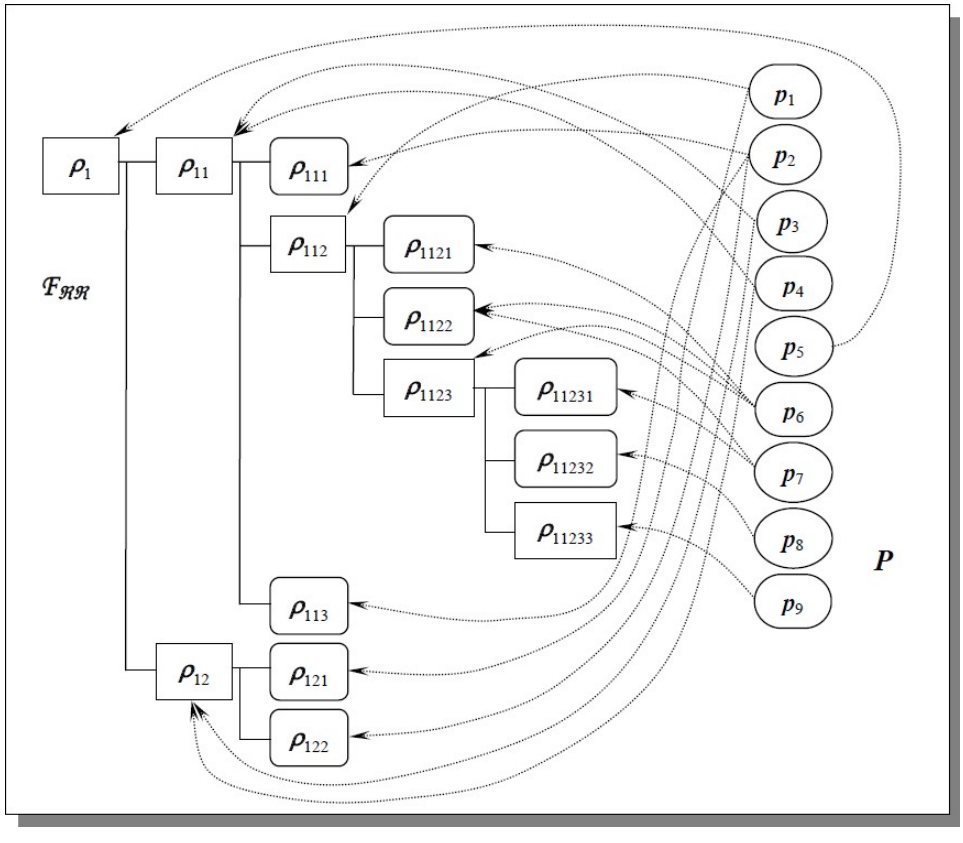
$$\mathbf{P(\rho_{11}) = P(\rho_{111}) \cup P(\rho_{112}) \cup P(\rho_{113}) =}$$

$$\mathbf{=p_1 \cup (P(\rho_{1121}) \cup P(\rho_{1122}) \cup P(\rho_{1123})) \cup p_5 =}$$

$$\mathbf{= p_1 \cup ((p_1 \cup p_2) \cup (p_1 \cup p_3) \cup (p_1 \cup p_4) \cup p_5 = p_1 \cup p_2 \cup p_3 \cup p_4 \cup p_5}$$

Задача № 7.2.

Пусть имеется система иерархически организованных ролей $\Re$ ***(ρ*∈$\Re$),** представленная на рис.



Ролям назначены полномочия из конечного множества P ($p \in P$).

Определить тип наделения ролей полномочиями (листовой таксономический, листовойнетаксономический, иерархически охватный).

Определить полномочия роли ρ_{11}.

Решение.

Ввиду того, что полномочия непосредственно назначаются и листовым и узловым ролям, то имеемиерархически охватный подход.

$P(\rho_{11}) = p_3 \cup p_4 \cup (P(\rho_{111}) \cup P(\rho_{112}) \cup P(\rho_{113}))=$

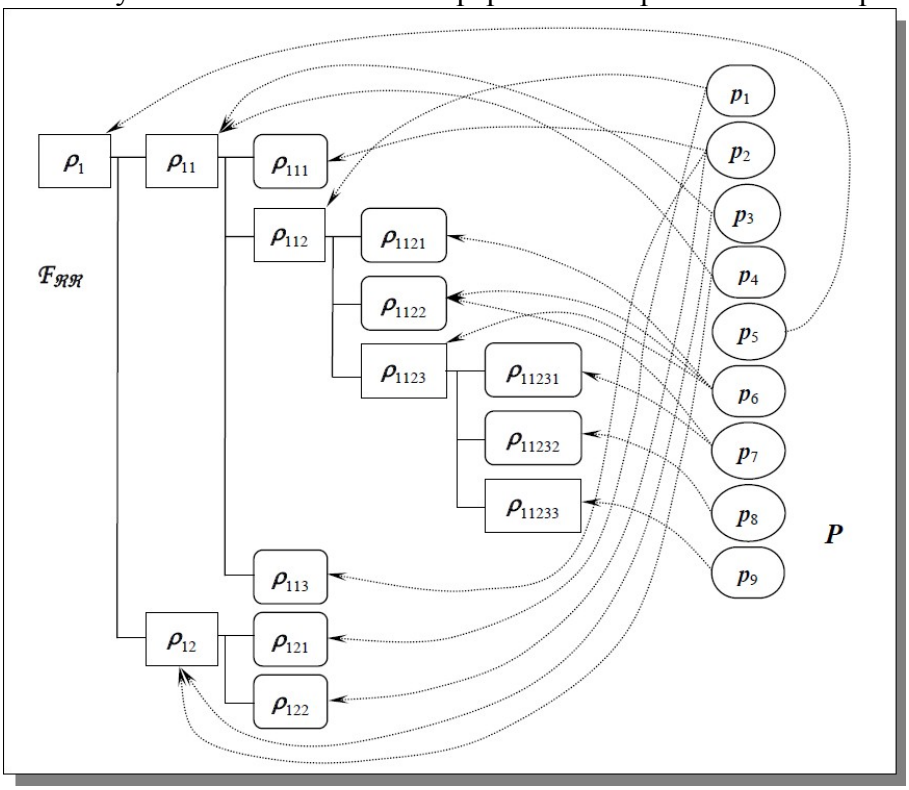
$=p_3 \cup p_4 \cup (p_2 \cup (p_1 \cup (P(\rho_{1121}) \cup P(\rho_{1122}) \cup P(\rho_{1123}))) \cup p_2) =$

$=p_3 \cup p_4 \cup (p_2 \cup (p_1 \cup (p_6 \cup (p_6 \cup p_7) \cup (p_6 \cup (p_7 \cup p_8 \cup p_9)))) \cup p_2=$

$= p_1 \cup p_2 \cup p_3 \cup p_4 \cup p_6 \cup p_7 \cup p_8 \cup p_9$

Задача № 7.3.

Пусть имеется система иерархически организованных ролей $\Re$ ($\rho \in \Re$), представленная на рис.



($p \in P$)Ролям на основе иерархически охватного подхода назначены полномочия из конечного множества P

При предположении, что определенные полномочия могут быть назначены только ролям определенного уровня иерархии, определить возможный порядок (отношение доминирования) на множестве полномочий.

Решение.

Будем исходить из того, что одно полномочие p_1 доминирует над другим полномочием ($p_2 \leq p_1$), если роль, которой назначено второе полномочие ρ_2, в иерархии ролей находится в подчинении первой роли ρ_1 (прямо или по дереву ролей) - $\rho_2 \leq \rho_1$.

Тогда определение порядка полномочий будем производит от полномочий корневой роли и т.д. вниз по иерархии ролей.

Первый уровень полномочий - p_5.

Второй уровень полномочий - p_3,

p_4. Третий уровень полномочий -

p_1, p_2. Четвертый уровень

полномочий - p_6, p_7.Пятый уровень

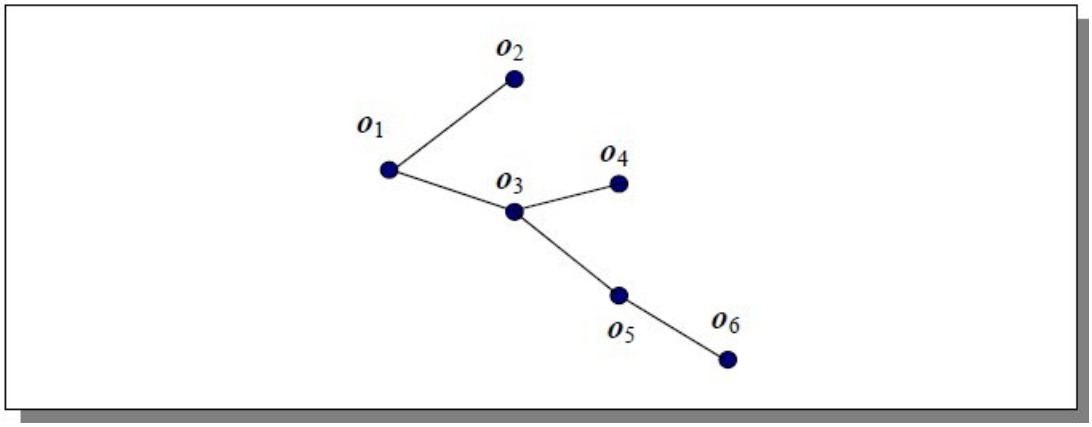
полномочий - p_7, p_8, p_9.

Следует обратить внимание, что порядок на множестве полномочий частичный и нелинейный. Такполномочие p_7 назначено одновременно ролям ρ_{1122} и ρ_{11231}.

Тема: Модель анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа

Задача № 8.1.

Пусть имеется иерархически организованная система объектов доступа.



Составить матрицу смежности объектов доступа **H** (строка – куда; столбец – кто входит; диагональныеэлементы равны 0) и матрицу итоговой достижимости $\mathbf{H^S}$ (за один шаг, за два шага и т.д.).

Решение.

$$H = \begin{array}{c|cccccc} & o_1 & o_2 & o_3 & o_4 & o_5 & o_6 \\ o_1 & 0 & 1 & 1 & 0 & 0 & 0 \\ o_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_3 & 0 & 0 & 0 & 1 & 1 & 0 \\ o_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_5 & 0 & 0 & 0 & 0 & 0 & 1 \\ o_6 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

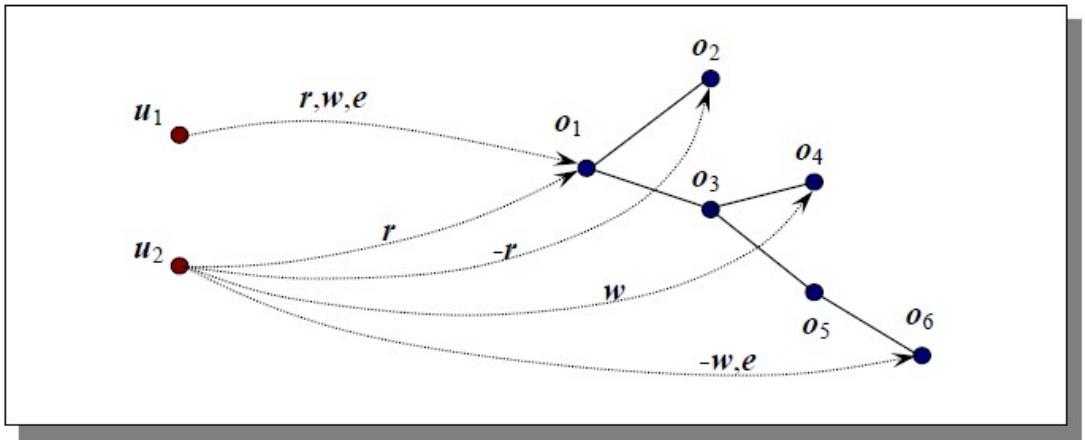
$$H^2 = \begin{array}{c|cccccc} & o_1 & o_2 & o_3 & o_4 & o_5 & o_6 \\ o_1 & 0 & 0 & 0 & 1 & 1 & 0 \\ o_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_3 & 0 & 0 & 0 & 0 & 0 & 1 \\ o_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_5 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_6 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$H^3 = \begin{array}{c|cccccc} & o_1 & o_2 & o_3 & o_4 & o_5 & o_6 \\ o_1 & 0 & 0 & 0 & 0 & 0 & 1 \\ o_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_5 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_6 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$$H^S = H + H^2 + H^3 = \begin{array}{c|cccccc} & o_1 & o_2 & o_3 & o_4 & o_5 & o_6 \\ o_1 & 0 & 1 & 1 & 1 & 1 & 1 \\ o_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_3 & 0 & 0 & 0 & 1 & 1 & 1 \\ o_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ o_5 & 0 & 0 & 0 & 0 & 0 & 1 \\ o_6 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Задача № 8.2.

Пусть имеется иерархически организованная система объектов доступа и два пользователя u_1и u_2,Назначения доступа показаны на рис.



Определить итоговые права доступа.

Решение.

Имеем следующие матрицы прав доступа по непосредственным назначениям.

R_r =

	o_1	o_2	o_3	o_4	o_5	o_6
u_1	1	0	0	0	0	0
u_2	1	-1	0	0	1	0

R_w =

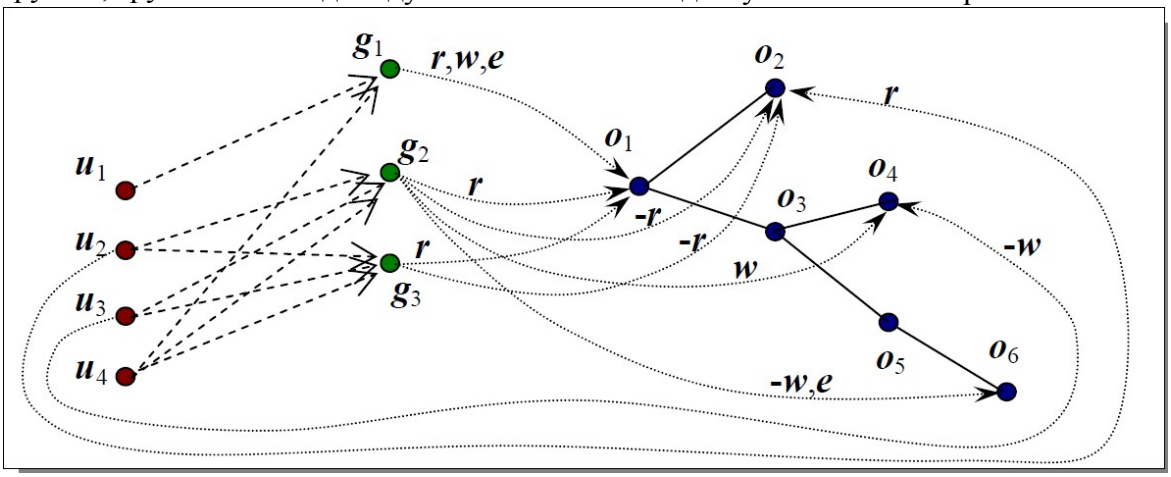
	o_1	o_2	o_3	o_4	o_5	o_6
u_1	1	0	0	0	0	0
u_2	0	0	0	0	0	-1

R_e =

	o_1	o_2	o_3	o_4	o_5	o_6
u_1	1	0	0	0	0	0
u_2	0	0	0	0	0	1

Задача № 8.3.

Пусть имеется иерархически организованная система объектов доступа, четыре пользователя ***u*₁, *u*₂, *u*₃** и ***u*₄**, объединенных в три рабочих группы ***g*₁, *g*₂** и ***g*₃**. Вхождение пользователей в рабочие группы, групповые ииндивидуальные назначения доступа показаны на рис.



Задание. Определите общий коэффициент дублирования прав доступа в системе по чтению и коэффициент дублирования прав доступа по чтению для пользователя ***u*₂**.

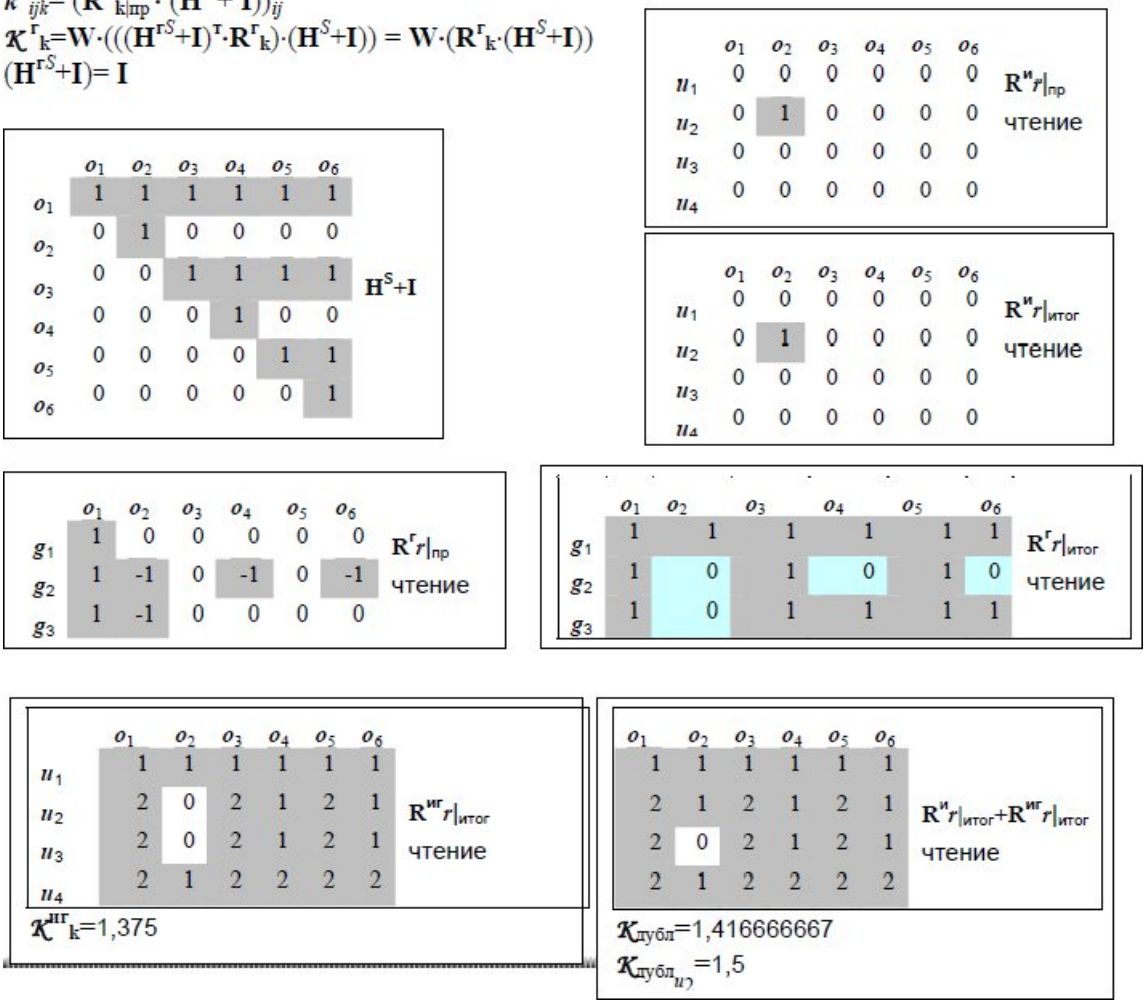
Решение.

$$К_{дубл}=(К^{и}_{k} + К^{иг}_{k})/N*M$$

$$k^{и}_{ijk}= (R^{и}_{k|пр} \cdot (H^{S} + I))_{ij}$$

$$К^{r}_{k}=W\cdot(((H^{rS}+I)^{т}\cdot R^{r}_{k})\cdot(H^{S}+I)) = W\cdot(R^{r}_{k}\cdot(H^{S}+I))$$

$$(H^{rS}+I)= I$$



5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

5.1.1. Перечень основной литературы:

1. Современные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / И.А. Королькова / А.Р. Ванютин / А.П. Алексеев ; ред. А.П. Алексеев. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2016. - 101 с. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Адлер, Ю.П. Статистическое управление процессами. «Большие данные» Электронный ресурс : учебное пособие / Е.А. Черных / Ю.П. Адлер. - Статистическое управление процессами. «Большие данные»,2019-09-01. - Москва : Издательский Дом МИСиС, 2016. - 52 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

5.1.2. Перечень дополнительной литературы:

1. Современные информационные технологии Электронный ресурс : Сборник трудов по материалам 3-й межвузовской научно-технической конференции с международным участием 29 сентября 2017 г. / В. И. Воловач [и др.] ; ред. В. М. Артюшенко. - Королёв : Научный консультант, МГОТУ, 2017. - 191 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Современные мультимедийные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / А.П. Алексеев / А.Р. Ванютин / И.А. Королькова. - Современные мультимедийные информационные технологии,2019-05-

25. - Москва : СОЛОН-ПРЕСС, 2017. - 108 c. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

5.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации по выполнению лабораторных работ по дисциплине " МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ "

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ "

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы по дисциплине «МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

для студентов направления подготовки **10.03.01 Информационная безопасность** направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2025

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

− формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
− написание докладов;
− подготовка к семинарам, практическим и лабораторным работам, их оформление;
− составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
− выполнение учебно-исследовательских работ, проектная деятельность;
− подготовка практических разработок и рекомендаций по решению проблемной ситуации;
− выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
− компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
− выполнение курсовых работ (проектов) в рамках дисциплин;
− выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «МЕТОДЫ ОЦЕНКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ» направлена на формирование следующих **компетенций**:

Код	Формулировка:
П К - 5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям	ИД-1 ПК-5 Знает нормативную документацию по аттестации объектов информатизации. ИД-2 ПК-5 Способен выполнять требования безопасности хранения и обработки информации. ИД-3 ПК-5 Обладает навыками аттестации объектов информации по средствам требований информатизации
П К - 9 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИД-1 ПК-9 Знает методы поиска научно-технической информации. ИД-2 ПК-9 Способен выбирать необходимую информацию в области информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности. ИД-3 ПК-9 Владеет навыками изучения научно-технической литературы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
П К - 1 0 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ИД-1 ПК-10 Понимает международные и отечественные стандарты соответствия объектов информационной безопасности. ИД-2 ПК-10 способен применять стандарты при анализе на соответствие объектов информационной безопасности. ИД-3 ПК-10 Владеет методами проведения анализа объектов информационной безопасности.
П К - 1 1 Способность проводить эксперименты по заданной	ИД-1 ПК-11 Знает методы обработки и анализа результатов проведения экспериментов. ИД-2 ПК-11 Умеет выбирать необходимые методы для обработки и анализа результатов проведения экспериментов. ИД-3 ПК-11 Владеет навыками обработки и анализа результатов

методике, обработку, оценку погрешности и достоверности их результатов	проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов.
П К - 1 2 Способность принимать участие в проведении экспериментальн ых исследований системы защиты информации	ИД-1 ПК-12 Понимать принципы функционирования системы защиты информации. ИД-2 ПК-12 способен проводить исследования описывая каждый этап эксперимента и обосновывать полученный результат. ИД-3 ПК-12 Владеет методами анализа процедуры исследования и результата согласно заданным критериям.

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
4 семестр					
ПК-5, ПК-9, ПК-10, ПК-11, ПК-12	Подготовка к лекциям	Собеседование	3,24	0,36	3,6
ПК-5, ПК-9, ПК-10, ПК-11, ПК-12	Самостоятельное изучение литературы по темам	Собеседование	22,68	2,52	25,2
ПК-5, ПК-9, ПК-10, ПК-11, ПК-12	Подготовка к практическим работам	Отчет письменный	6,48	0,72	7,2
Итого за 4 семестр			**32,4**	**3,6**	**36**
Итого			**32,4**	**3,6**	**36**

Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной

последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно,

исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на	Обнаруживаются	Студент	Проект

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	некоторые ошибки в использовании соответствующих технических средств и информационных технологий	достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него

не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. 1. eLIBRARY.Ru [Электронный ресурс]: электронная библиотека / Науч. электр. б- ка.- МОСКВА.1999. – Режим доступа: http//elibrary.ru (дата обращения 15.03.2020). – Яз. рус., англ.

2. Moodle [Электронный ресурс]: система виртуального обучения:[база данных] / Даг.гос.универ. – Махачкала, - Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http: //moodl.dgu.ru. (дата обращения 22.01.20).

3. Электронный каталог НБ ДГУ Ru [Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа: http//elib.dgu.ru. свободный (дата обращения 11.03.2020)

4. Национальный Открытый Университете «ИНТУИТ» [Электронный ресурс]: - www.intuit.ru (дата обращения 12.03.2020)**Дополнительная литература:**

1. Современные информационные технологии Электронный ресурс : Сборник трудов по материалам 3-й межвузовской научно-технической конференции с международным участием 29 сентября 2017 г. / В. И. Воловач [и др.] ; ред. В. М. Артюшенко. - Королёв : Научный консультант, МГОТУ, 2017. - 191 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Современные мультимедийные информационные технологии Электронный ресурс : учебное пособие / С.С. Мытько / Д.А. Репечко / А.П. Алексеев / А.Р. Ванютин / И.А. Королькова. - Современные мультимедийные информационные технологии,2021-05-25. - Москва : СОЛОН-ПРЕСС, 2017. - 108 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации для самостоятельной работы студентов по дисциплине «Практическая работа»
2. Методические указания к лабораторным работам по дисциплине «Практическая работа»

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Практическая работа»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.