ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Заведующий кафедрой

_____

«___» _____20__ г.

Методическая разработка и указания к практическим занятиям по дисциплине «Информационные технологии в управлении» (для всех профилей подготовки)

Тема №2 Программное и техническое и обеспечение сетевых коммуникаций

<u>Практическое занятие №2</u>«Управление доступом к данным»

Рассмотрено УМК
«___» _____20__ г.
Протокол №____
Председатель УМК
_____

Ставрополь, 2022

Рецензент:
доктор технических наук, профессор Федоренко В.В.

Одобрено учебно-методической комиссией экономического факультета Ставропольского государственного аграрного университета

Методические указания к практическим занятиям разработаны в соответствии с программой курса «Информационные технологии в управлении»

Составитель:
Доцент, к.т.н., доцент Рачков В.Е.

СОДЕРЖАНИЕ:

1. Меры безопасности при работе на компьютере

Конструкция компьютера обеспечивает электробезопасность для работающего на нем человека. Тем не менее, компьютер является электрическим устройством, работающим от сети переменного тока напряжением 220 В., а в мониторе напряжение, подаваемое на кинескоп, достигает нескольких десятков киловольт. Чтобы предотвратить возможность поражения электрическим током, возникновения пожара и выхода из строя самого компьютера при работе и техническом обслуживании компьютера необходимо соблюдать следующие меры предосторожности:

- сетевые розетки, от которых питается компьютер, должны соответствовать вилкам кабелей электропитания компьютера;
- запрещается использовать в качестве заземления водопроводные и газовые трубы, радиаторы и другие узлы парового отопления;
- запрещается во время работы компьютера отключать и подключать разъемы соединительных кабелей;
- запрещается снимать крышку системного блока и производить любые операции внутри корпуса до полного отключения системного блока от электропитания;
- запрещается разбирать монитор и пытаться самостоятельно устранять неисправности (опасные для жизни высокие напряжения на элементах схемы монитора сохраняются длительное время после отключения электропитания);
- запрещается закрывать вентиляционные отверстия на корпусе системного блока и монитора посторонними предметами во избежание перегрева элементов расположенных внутри этих устройств;
- повторное включение компьютера рекомендуется производить не ранее, чем через 20 секунд после выключения.

2 Введение

В практическое занятие включены индивидуальные задания по Теме №2 «Программное и техническое и обеспечение сетевых коммуникаций».

Материалы практического занятия дополняют лекционный курс и на практике рассматриваются организация процессов, различные способы их взаимодействия, устройство файловой системы, системы доступа к данным.

1. УПРАВЛЕНИЕ ДОСТУПОМ К ДАННЫМ ОПЕРАЦИОННОЙ СИСТЕМЫ

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). Речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в вид матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Таблица 1 Фрагмент матрицы доступа

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

"o" - обозначает разрешение на передачу прав доступа другим пользователям,
"r" - чтение,
"w" - запись,
"e" - выполнение,
"a" - добавление информации

Тема логического управления доступом - одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект - это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;
- атрибуты субъекта (метка безопасности, группа пользователя и т.п.).

Метки безопасности – основа принудительного (мандатного) управления доступом.

Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить

доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются списки управления доступом). К сожалению, у "произвольного" подхода есть ряд недостатков. ***Рассредоточенность управления доступом*** ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что ***права доступа существуют отдельно от данных***. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование и пользовательская работа.

Практическое занятие №2
«Управление доступом к данным»

1. Изучить приемы работы со справочной системой Windows 10.
2. Изучить последовательность действий пользователя при управлении доступом к данным.
3. Разработать алгоритм действий пользователя при организации управления доступом к данным. Алгоритм представить в виде презентации, отражающий последовательность действий пользователя.

Время: 2 часа.

Место проведения: Компьютерный класс

Методическое обеспечение работы:

1. ПЭВМ с установленной операционной системой Windows 7/10;
2. Методические указания к практическим занятиям по теме №2 «Программное и техническое и обеспечение сетевых коммуникаций».

Порядок проведения практического занятия

1. Изучить приемы работы со справочной системой Windows 7/10.

Пользуясь справочной системой Windows провести поиск раздела определяющего процедуры управления доступом к данным.

2. Подготовить алгоритм действий пользователя при организации доступа к данным (в соответствии с выданным вариантом.

Пользуясь сведениями справочной системы Windows подготовить в среде PowerPoint презентационный проект, отражающий последовательность действий пользователя при организации работы службы операционной системы.

4. Представить подготовленную презентацию для проверки и защиты преподавателю.

Студенты готовят презентации, отражающие последовательность действий пользователей, размещают их в своих личных кабинетах в папках соответствующих номеру практического занятия и отправляют ссылку преподавателю на размещенный ресурс.

Варианты индивидуальных заданий
к практическому занятию №4

№ варианта	Действия пользователей
1.	Работа с сетевыми файлами в автономном режиме
2.	Открытие файла или папки
3.	Доступ к файлам и принтерам на других компьютерах домашней группы
4.	Поиск файлов и папок на других компьютерах в сети
5.	Предоставление общего доступа к корневому каталогу диска
6.	Защита определенных файлов и папок от общего доступа в домашней группе
7.	Совместное использование библиотек в домашней группе
8.	Отключение общего доступа к подключению Интернета
9.	Совместное использование зашифрованных файлов
10.	Переключение между домашней сетью и сетью на рабочем месте
11.	Использование общего доступа к подключению Интернета
12.	Совместное использование одного подключения к Интернету несколькими компьютерами

5. Список рекомендованных источников

1. Компьютерные сети: принципы, технологии, протоколы : учеб. пособие для студентов вузов: В.Г. Олифер, Н.А. Олифер. - 4-е изд. - СПб. : Питер, 2011. - 944 с.: ил.
2. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. 2-е изд. — СПб.: Питер, 2009. — 669 с.: ил.
3. Информатика. Базовый курс: учеб. пособие для студентов техн. вузов (для бакалавров и специалистов) / под ред. С.В. Симоновича. - 3-е изд. - СПб.: ПИТЕР, 2014. - 640 с.
4. Информатика и информационные технологии: конспект лекций / Ю. Д. Романова, И. Г. Лесничная. - 2-е изд., перераб. и доп. - М. : Эксмо, 2014. - 320 с.