УДК 004.588
DOI 10.21685/2587-7704-2018-3-2-1

Open Access | RESEARCH ARTICLE

Обучающая система по разграничению прав доступа в операционной системе Windows

В. В. Исмаилов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

М. Ю. Лупанов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Статья посвящена актуализации и решению основных проблем, связанных с определением и созданием программного комплекса, предназначенного для обучения пользователей теоретическим и практическим навыкам разграничения доступа к объектам в операционной системе Windows. Рассмотрены основные функции Windows API, которые необходимы при создании программного комплекса. Определен состав и содержание комплекса. Главное достоинство программного комплекса – автоматизация процесса обучения и повышение мотивации и интереса к обучению у пользователей.

Ключевые слова: информация, информационная безопасность, автоматизированная обучающая система, защита информации, обучение, разграничение доступа.

Training system for access rights differentiation in Windows operating system

V. V. Ismailov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

M. Yu. Lupanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article is devoted to the actualization and solution of the main problems associated with determination and creation of a software package designed to develop users' theoretical and practical skills in access differentiation to objects in the Windows operating system. The main functions of the Windows API, which are necessary when creating a software package, are considered. The composition and content of the package has been determined. The main advantage of the software package is the automation of the training process and promoting users' motivation and interest for training.

Keywords: information, information security, automated training system, information protection, training, access differentiation.

Целью данной статьи является актуализация и решение основных проблем, связанных с определением и созданием программного комплекса, предназначенного для обучения пользователей теоретическим и практическим навыкам разграничения доступа к объектам в операционной системе Windows.

В сфере информационных технологий одной из главных проблем всегда являлась защита информации. Появляются новые технологии хранения, передачи и получения информации, а значит, с годами проблема защиты информации не теряет своей актуальности.

Одним из способов защиты информации от несанкционированного доступа является разграничение доступа. Знание теоретических основ методов разграничения доступа вместе с практическими навыками их применения формирует уверенность при применении такого способа защиты информации.

Необходимые знания и навыки формируются в результате процесса обучения, эффективность которого можно повысить, используя компьютерные технологии. С их помощью можно создавать автоматизированные обучающие системы, которые повышают интерес и стимулируют процесс обучения.

Актуальность создания автоматизированной обучающей системы заключается в том, что знания и умения, полученные в результате применения разрабатываемой системы, способствуют решению проблемы защиты информации.

В операционных системах Windows реализована дискреционная модель безопасности. В качестве активных субъектов этой модели безопасности рассматриваются процессы и потоки, каждый из которых работает от имени некоторого пользователя. Когда пользователь регистрируется и входит в систему, то для него создается маркер доступа (accesstoken), который идентифицирует этого пользователя и содержит его привилегии. Каждый процесс, исполняемый от имени пользователя, имеет маркер доступа этого пользователя. Маркер доступа используется для контроля доступа процесса к объектам, которые называются в Windows охраняемыми объектами (securableobjects). К охраняемым объектам относятся все объекты Windows, которые могут иметь имя. Кроме того, к охраняемым объектам относятся также потоки и процессы. Каждый охраняемый объект имеет дескриптор безопасности (securitydescriptor), который создается вместе с охраняемым объектом и содержит информацию, необходимую для защиты объекта от несанкционированного доступа. В дескрипторе безопасности идентифицируется владелец объекта, определяются пользователи и группы пользователей, которым разрешен или запрещен доступ к охраняемому объекту, а также информация для аудита доступа к объекту. Изменять информацию, заданную в дескрипторе безопасности, может только владелец объекта, которым по умолчанию является создатель этого объекта. При доступе к охраняемому объекту система сверяет информацию о пользователе, заданную в маркере доступа, с информацией, заданной в дескрипторе безопасности. Если в дескрипторе безопасности указано, что пользователю разрешен доступ к объекту, то процесс получает запрашиваемый доступ, в противном случае в доступе отказывается.

Для хранения информации о пользователях, которым разрешен или запрещен доступ к охраняемым объектам, каждый дескриптор безопасности содержит список управления дискреционным доступом (DiscretionaryAccess-ControlList, DACL). Для управления аудитом доступа к объекту в дескрипторе безопасности хранится список управления системным доступом (SystemAccess-ControlList, SACL). Общее название для этих списков – списки управления доступом (Access-ControlLists), или сокращенно ACL.

Таким образом, можно сказать, что в операционных системах Windows NT/2000/XP реализована дискреционная модель безопасности, в которой управление правами доступа к объекту выполняет владелец этого объекта.

Каждый охраняемый объект в операционных системах Windows имеет дескриптор безопасности, который используется операционной системой для ограничения доступа к этому объекту.

Для получения дескриптора безопасности объекта по имени этого объекта используется функция GetNamedSecurityInfo.

Из дескриптора безопасности можно получить список управления доступом к объекту DACL. Для получения этих данных используется функция GetSecurityDescriptorDacl.

Основные функции по созданию и удалению групп и пользователей:

– для создания/удаления учетной записи пользователя используются функции NetUserAdd/NetUserDel;

– для создания/удаления локальной группы используется функция NetLocalGroupAdd/ NetLocalGroupDel;

– для добавления/удаления членов локальной группы используется функция NetLocalGroupDelMembers/NetLocalGroupAddMembers.

Список управления доступом к объекту DACL представляет собой соотношение идентификаторов SID и маски доступа. Для преобразования SID в имя группы или пользователя используется функция LookupAccountSid.

Для определения способов и методов обучения в первую очередь необходимо понять, что такое обучение и как достичь целей обучения. Обучение – это целенаправленный педагогический процесс организации и стимулирования активной учебно-познавательной деятельности учащихся по овладению знаниями, умениями и навыками.

Знания можно получить путем усвоения предоставленного теоретического материала, а умения и навыки в ходе выполнения практических заданий.

С помощью программного комплекса можно реализовать наглядные и практические методы обучения. К наглядным методам обучения относятся теоретические материалы по разграничению доступа, а к практическим – выполнение пользователем последовательности действий по ограничению доступа к объектам в Windows согласно сформированному заданию с автоматической проверкой правильности выполнения задания.

В результате постижения сущности методов разграничения доступа у пользователей формируются обобщающие выводы, которые укрепляются при выполнении практических заданий, что приводит к достижению цели обучения.

В программный комплекс могут быть включены следующие теоретические материалы для самостоятельного изучения:

- методы и способы разграничения доступа;
- методы разграничения доступа, применяемые в ОС Windows;
- способы управления доступом в ОС Windows.

Кроме теоретических материалов, программный комплекс предоставит возможность для практического освоения способов управления доступом в ОС Windows.

Практическую часть условно можно разбить на несколько этапов:

- формирование задания. На этом этапе создаются объекты и субъекты доступа, а также генерируется матрица доступа, определяющая набор прав каждого субъекта к каждому объекту;
- выполнение задания. Пользователю необходимо реализовать матрицу доступа в соответствии с заданием, а именно для каждого объекта определить, какие права имеет каждый субъект;
- завершение выполнения задания. На данном этапе производится автоматическая проверка результатов выполнения задания с отображением возможных ошибок. Проверка заключается в сравнении списка управления доступа из задания с фактически установленным списком для данных файлов в системе.

Программный комплекс может иметь клиент-серверную архитектуру, как показано на рис. 1.

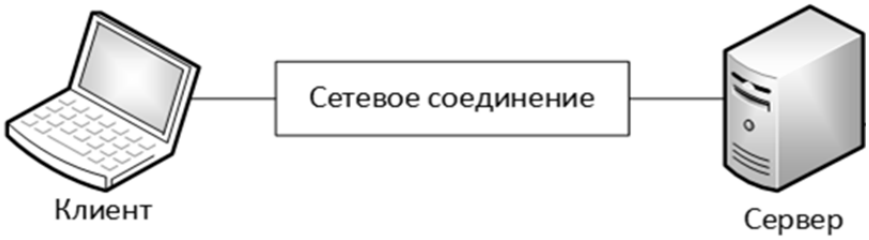

Рис. 1. Клиент-серверная архитектура

Такая архитектура позволяет упростить процесс контроля за обучением благодаря возможности реализации следующих функций:

- возможность параллельного выполнения практических заданий на нескольких рабочих местах, контролируемых сервером;
- автоматическая рассылка заданий по рабочим местам;
- автоматический сбор результатов выполнения практических заданий, их сортировка и хранение;
- автоматическое формирование отчетов по результатам практик;
- вывод статистических данных.

В данной статье предложены решения по основным проблемам при создании программного комплекса, предназначенного для обучения пользователей теоретическим и практическим навыкам разграничения доступа к объектам в операционной системе Windows.

Исмаилов, В. В.
Обучающая система по разграничению прав доступа в операционной системе Windows / В. В. Исмаилов, М. Ю. Лупанов // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-1.