

плазмонотронного резонанса. Спектры поглощения жидких коллоидных растворов определяли газовой фазой методом.

Ключевые слова: наночастица, сұйықталған коллоидты ерітінділер, поглощение, плазмон, плазмотронный резонанс, уровень Ферми, запрещенная зона, оптика.

Abstract

The article discusses the optical properties of semiconductor nanoparticles. The article investigates the optical properties of semiconductors in a nanosystem and the appearance of size effects with a decrease in the size of nano-objects. The quantum-size effect is taken into account when studying the sizes of nanostructures. The effect of quantum effects on the properties of nano-objects of various sizes was studied by the plasmonotron resonance method. The absorption spectra of liquid colloidal solutions were determined by the gas-phase method.

Key words: nanoparticles, colloidal solutions, absorption, plasmon, plasmonotron resonance, level of Fermi, restricted area, optics.

МРНТИ 14.35.09

¹Мухамбетова М.Ж., ²Серік М., ³Kultan J.

^{1,2} Евразийский национальный университет им.Л.Н.Гумилева,
г.Нур-Султан, Республика Казахстан

³Экономический университет в Братиславе
г. Братислава, Словацкая Республика

mukhambetovamj@gmail.com

ПУТИ ПРИМЕНЕНИЯ В УЧЕБНОМ ПРОЦЕССЕ ВУЗА МЕТОДОВ ЗАЩИТЫ КЛИЕНТ-СЕРВЕРНЫХ СИСТЕМ

Аннотация

В данной статье рассматриваются методы защиты клиент-серверных систем, и их применение в учебном курсе по клиент-серверным технологиям. Структура и методические аспекты внедрения модуля «Системы безопасности в серверных баз данных и организация подключения к данным» в учебном процессе вуза. Применение методов по настройке виртуальной частной сети, аутентификация в MS SQL Server, создание группы пользователей и управление их записями, роль серверов и базы данных, назначение ролей к базам данных и их объектам, резервное копирование, восстановление базы данных.

Ключевые слова: клиент-серверные системы, виртуальная частная сеть, аутентификация, безопасность, защита, учебный процесс, модуль.

На сегодняшний день безопасность является одним из главных функций всех систем программного обеспечения. Для эффективной работы современных предприятий, а также учебных учебных заведений важную роль играет хранение и передача дорогостоящих информации от несанкционированного доступа. В сущности многие понятия и термины относящихся к безопасности схожи. Проблемы безопасности клиент-серверных систем относятся к актуальным темам, и в процессе обучения будущих специалистов нужно уделять особое внимание этому вопросу. Для решения этой задачи в рамках курса по клиент-серверным технологиям мы внедрили модуль под названием «Системы безопасности в серверных базах данных и организация подключения к данным». Целью данного модуля является обучение студентов теоретическим знаниям в области защиты клиент-серверных систем и баз данных, а также способствовать формированию практических навыков к применению методов защиты. В нашем исследовании для разработки клиент-серверных систем использовалась платформа MS SQL Server [1]. В рамках указанного модуля рассматриваются следующие темы:

- настройка виртуальной частной сети и организация безопасности клиент-серверных систем;
- аутентификация MS SQL Server, создание группы пользователей и управление их записями;
- роль серверов и базы данных, назначение ролей к базам данных и их объектам;
- резервное копирование и восстановление базы данных.

Применение виртуальных частных сетей (VPN) в корпоративных клиент-серверных системах обеспечивает высокий уровень безопасности данных. VPN – объединяет географически разнесенные филиалы и передает поток данных через защитную сеть [2], [3]. Данная технология считается одним из востребованных, грамотных и экономически выгодных решений при реализации клиент-серверных систем [4]. Организация сети VPN обеспечивает защиту баз данных на сервере от несанкционированного использования и шпионских действий.

В нашем исследовании настройка виртуальной частной сети и процесс передачи данных в клиент-серверных системах использовалась в учебном процессе Казахских вузов и в вузе Центральной Европы, на базе кафедры «Прикладная информатика» Экономического университета в Братиславе [5].

Отражение тем в содержании учебных курсов по клиент-серверной технологии, способствует к ознакомлению обучающихся теоретическим основам виртуальных частных сетей и безопасности данных, а также формирует практические навыки администрирования и применения VPN.

На следующем рисунке можно представить все узлы подключенные к сети Интернет по Казахстану, и здесь можно увидеть филиалы одной компании объединенных по сети VPN (рисунок 1).

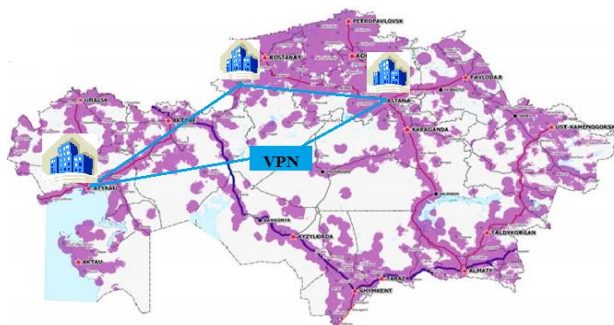


Рисунок 1 – Организация виртуальной частной сети

В качестве эффективного метода защиты данных практическая реализация настройки сети VPN в учебном процессе вуза осуществлялся следующим образом.

- установка программы LogMeIn Hamachi на узлах в сети;
- назначение новых IP-адресов на компьютерах в которых была установлена программа;
- проверка состояния обмена пакетами данных между компьютерами (с использованием команды ping);
- создание новой защищенной частной сети с одного узла, то есть с одного компьютера (рисунок 2);
- подключение других узлов к созданной частной сети;
- отключение брандмауэра для бесперебойной работы сети.

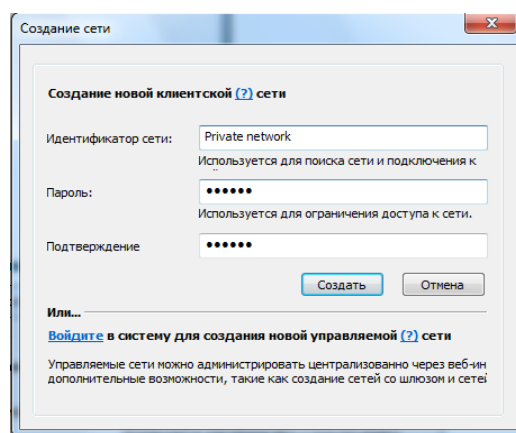


Рисунок 2 – Настройка новой VPN сети

В процессе реализации данного метода использовался групповая форма обучения. Так как для учебных целей использовалась бесплатная версия программы LogMeIn Hamachi, которая подключает до пяти узлов в

одной сети. Для корпоративных решений можно воспользоваться другими видами подписки к программе.

Обучение к применению виртуальных частных сетей в клиент-серверных системах, является предпосылкой для разработки и создания масштабных корпоративных информационных систем и высокопроизводительных облачных хранилищ.

Аутентификация - является еще одним методом защиты данных, которая управляет процессом проверки подлинности различных объектов. Ресурсы считаются защищаемыми объектами, доступ к которым производится через аутентификацию. Архитектура безопасности платформы MS SQL Server имеет ряд принципов, с которыми нужно ознакомиться перед конфигурированием отдельных параметров. Некоторые из защищаемых объектов, могут храниться внутри других защищаемых объектов. К ним относятся сервер, база данных и схема [6], [7].

На следующем рисунке отображены защищаемые объекты на уровне сервера в MS SQL Server (рисунок 3).



Рисунок 3 - Защищаемые объекты на уровне сервера в MS SQL Server

К защищаемым объектам на уровне базы данных относятся следующие:

- Схема;
- Роль приложения;
- Сборка;
- Асимметричный ключ;
- Сертификат;
- Контракт;
- Полнотекстовый каталог;
- Привязка удаленной службы;
- Тип сообщений;
- Роль (базы данных);
- Маршрут;
- Поиск в списке свойств;

- Служба;
- Понотекстовый список стоп-слоев;
- Симметричный ключ;
- Пользователь.

При создании нового имени для входа пользователя назначаются роли сервера и базы данных. Для этого нужно учесть привилегий предусмотренные в MS SQL Server (рисунок 4).

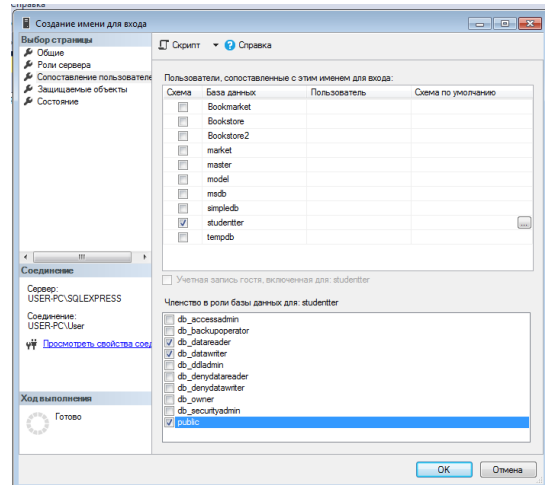


Рисунок 4 – Окно назначения ролей и привилегий для пользователя базы данных

Метод резервного копирования данных обеспечивает восстановление базы данных в случае сбоя. В MS SQL Server существует несколько типов резервных копий, как полная (full), разностная (differential), копия журнала транзакций (transaction log), копия файлов и файловых групп (file/file group), частичная (partial) и копия только для копирования (copy only) [8]. Большой набор резервных копий предоставляет широкий выбор вариантов, чтобы помочь оптимизировать процесс. Здесь также можно использовать возможности сжатия и шифрования данных.

Для восстановления базы данных используется три типа моделей. Выбор модели реализуется в окне *Свойства* базы данных – страницы *Параметры*. В случае возникновения аварии все модели сохраняют данные, но каждая модель восстановления имеет свои особенности.

В рамках данной статьи были обсуждены основные моменты использования методов для безопасности и защиты данных. Каждый вид из указанных направлений имеет свои особенности и привилегий. Но общее назначение всех методов направлено на защиту клиент-серверных систем, обеспечение успешной и бесперебойной работы.

Надеемся, что владение обучающихся вышеуказанными методами способствует решению профессиональных задач в их будущей карьере.

Список литературы:

1. Серік М., Мухамбетова М.Ж., Култан Я. «Клиент-сервер технологиясы» курсы бойынша жоғары оқу орнында білім берудің дидактикалық негіздері туралы // Л.Н. Гумилев атындағы Еуразия Ұлттық университетінің хабаршысы. Педагогика. Психология. Әлеуметтану сериясы. - №4 (125) / 2018, 68-74 б.
2. Шейда В. В. Использование протоколов TCP и UDP для защищенной передачи информации по SSL-VPN-туннелям // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – №. 1-2 (21). – С. 225-230.
3. Герасимова О. Ю., Мингалеева Л. Б. Технологии объединения территориально удаленные филиалы учебных заведений в единую корпоративную сеть // In the World of Scientific Discoveries/V Mire Nauchnykh Otkrytiy. – 2015. – Т. 72. – С. 10-127
4. Березин А., Петренко С. Построение корпоративных защищенных виртуальных частных сетей // Сетевой журнал. – 2001. – №. 1. – С. 7-11.
5. Kultan J., Schmidt P., Mukhambetova M. Distributed Data Processing in the Economy // Economics, Management and Technology in Enterprises 2019 (EMT 2019). – Atlantis Press, 2019. – p. 6-8.
6. Серік М. Клиент-сервер технологиясын жүзеге асыру (SQL Ортасы): оқу құралы. – Астана, Л.Н. Гумилев атындағы ЕҰУ, 2015. - 93 б.
7. Осетрова И.С. Администрирование SQL Server 2014. – С.110
8. Исаев Е. А., Корнилов В.В., Тарасов В.А., Детков Г.В. Использование трехзвенной архитектуры" клиент-сервер" в современных системах обработки информации // Известия Института инженерной физики. – 2015. – Т. 3. – №. 37. – С. 38-43.

Аңдатпа

Бұл мақалада клиент-серверлік жүйелерді қорғау әдістері және оларды клиент-сервер технологиялары бойынша оқу курсына қолдану жолдары баяндалады. ЖОО оқу үдерісіне енгізілген «Серверлік деректер қорындағы қауіпсіздік жүйелері және деректерге қосылуды ұйымдастыру» модулінің құрылымы мен оны жүзеге асырудың әдістемелік негіздері, виртуалды жеке желіні күйге келтіру, MS SQL Server аутентификациясы, пайдаланушылар тобын құру және олардың жазбаларын басқару, серверлер мен деректер қорының рөлдері, резервті көшірме алу және деректер қорын қалпына келтіру әдістері сипатталады.

Негізгі сөздер: клиент-серверлі жүйе, виртуалды жеке желі, аутентификация, қауіпсіздік, қорғау, оқу үдерісі, модуль.

Abstract

In this article discusses methods for protecting client-server systems, and their application in the training course on client-server technologies. Structure and methodological aspects of the implementation in the educational process of high education the module "Security systems in server databases and organization of data connection". Applying of methods for setting up a virtual private network , authentication in MS SQL Server, creating a group of users and managing their records, the role of servers and databases, assigning roles to databases and their objects, backup, database recovery.

Key words: client-server systems, virtual private network, authentication, security, protection, training process, module.