Одним из основных способов продвижения товара на рынок является реклама. Первым шагом будет распространение информации об открытии магазина. В этот день будет проведена акция, например, бесплатная установка дополнительного оборудования на технику.

1. Беспалов, М.В. Особенности развития предпринимательской деятельности в условиях современной России [Текст] / М.В. Беспалов. – М. ИНФРА-М, 2014. – 232 с.
2. Липсиц, И. В. Что такое бизнес-план и как его составить [Текст] / И.В. Липсиц. – М.: Россия молодая, 2011. – 387 с.
3. Степанов, И.М. Бизнес-планы. Полное справочное руководство [Текст] / И.М. Степанов – М.: Лаборатория базовых знаний, 2011. – 240 с.
4. Аликаева М.В. Бизнес планирование инвестиционного проекта. // Финансы С Бочаров В.В. Методы финансового моделирования. М.: Финансы и статистика, 2008 г. 45 с. 3.
5. Вдовенко Л.Л. Системно информационный подход к оценке экономической деятельности промышленных предприятий. М.: Экономическое образование, Информационные системы в экономике / Под ред. В.В. Дика. М.: Финансы и статистика,
6. Методологические рекомендации, по оценке эффективности инвестиционных проектов. М., Информэлектро, с. 7.

Асейдулин И.Р.

Анализ стратегии информационной безопасности и защиты компьютерных сетей

*Самарский государственный технический университет
(Россия, Самара)*

doi: 10.18411/lj-07-2020-62

idsp: ljjournal-07-2020-62

Аннотация

Компьютеры тесно связаны с нашей жизнью и работой. Однако они не являются абсолютно безопасными, и время от времени происходят случаи кражи информации. Для решения этих проблем существует множество технологических уровней, таких как технология криптографии, сетевой безопасности. В целях обеспечения нормальной работы компьютерных сетей, обеспечения информационной безопасности и предотвращения утечки и хищения информации создана специальная система защиты, обеспечивающая безопасность информации компьютерной сети путем обнаружения посторонних компьютеров, оценки безопасности. Однако с быстрым развитием техники, обновление электронных продуктов происходит все быстрее и быстрее, а проблема обеспечения сетевой безопасности информации становится все более серьезной.

Ключевые слова: информационные системы, информационная компьютерная сеть, информационная безопасность, защита информации

Abstract

Computers are closely linked to our lives and work. However, they are not completely secure, and from time to time, there are cases of information theft. To solve these problems, there are many technological levels, such as cryptography and network security technology. In order to ensure the normal operation of computer networks, ensure information security and prevent leakage and theft of information, a special protection system has been created to ensure the security of computer network information by detecting unauthorized computers and evaluating security. However, with the rapid development of technology, the update of electronic products is happening faster and faster, and the problem of ensuring network security of information is becoming more serious.

Keywords: information systems, information computer network, information security, information protection

Хранение массивных данных также создает определенные проблемы для компьютерных технологий. Многие технологии и инструменты информационной безопасности нуждаются в срочном решении. Традиционные информационные технологии не в состоянии удовлетворить потребности в хранении массивных данных. В настоящее время наиболее заметными и серьезными проблемами компьютерной информационной безопасности в эпоху больших данных являются кража данных, неправильное добавление и удаление данных, а также фальсификация, раскрытие личной тайны и так далее. Процесс защиты компьютерной информационной безопасности требует, чтобы все виды стратегий использовались совместно и были разумно развернуты. Только так мы сможем минимизировать вероятность нарушения информационной безопасности и получить гарантии безопасности.

На данный момент существует достаточно большое количество потенциальных угроз информационной безопасности. Перечислим один из самых основных из них: подмена платежной системы на стороннюю платежную систему злоумышленников; вирусные программы; DDoS атаки; атаки на электронную почту; социальная инженерия; загрузка постороннего программного обеспечения; хакерские атаки. Далее перейдем к рассмотрению стратегии защиты информационной безопасности компьютерных сетей.

В компьютерной сети существует много видов учетных записей. Когда в сетевой системе возникают проблемы с безопасностью или отклонения, злоумышленники часто крадут данные учетной записи пользователя. Поэтому пользователи сети должны увеличивать сложность пароля учетной записи (добавить сочетание цифр, букв и других символов). Продумывание, а не использование простых цифр или букв в качестве паролей, поможет сделать сеть более закрытой и надёжной. Также не следует использовать один и тот же пароль для разных учетных записей.

В настоящее время программное обеспечение брандмауэра установлено в большинстве компьютерных сетей. Он может сканировать ресурсы сетевого доступа в компьютерной системе, находить и решать скрытые проблемы безопасности в системе, а также эффективно контролировать доступ между различными сетями, чтобы избежать использования пользовательской компьютерной системы другими сетями. [1] Атаки на информационные технологии, например, когда пользователи используют компьютерные сети для просмотра соответствующих веб-страниц и обработки некоторых сетевых данных, могут использовать соответствующие стратегии безопасности для защиты своей собственной информационной безопасности. Когда сеть работает, брандмауэр также может внимательно отслеживать информацию о сети и автоматически отказываться принимать информацию о данных с риском. Брандмауэры обычно используют IP-адрес пользователей сети для поиска опасной информации о данных. Их функция управления может преобразовывать IP-адрес пользователей. Это может гарантировать, что они могут скрывать точные и реальные IP-адреса при управлении внутренней сетью, что затрудняет вход внешней атакующей сети во внутреннюю базу данных для уничтожения.

Технология так называемых «защитных стен», является эффективным способом обеспечения информационной безопасности компьютерной сети. Таким образом, в эпоху больших данных для работы компьютерной сети следует усилить эффективное использование защитной стены или системы безопасности [2]. Например, в корпоративном компьютерном приложении задействованная информация не только велика, но и очень важна. По этой причине на предприятии должна быть создана совершенная система предотвращения информационной безопасности данных, позволяющая главным образом повысить осведомленность управленческого персонала о безопасности компьютерных сетей. Особенно в условиях эпохи больших данных. Чтобы эффективно избежать влияния вирусов и хакерских атак на безопасную работу компьютерных сетей, необходимо усилить использование технологии брандмауэра для вмешательства в вредоносное программное обеспечение.

Технология «защитных стен» играет эффективную роль в изолировании вирусов, а использование топологической структуры может эффективно повысить безопасность и надежность работы компьютерной сети. В настоящее время, с непрерывным развитием компьютерных технологий, характеристики и стили вирусов становятся все более разнообразными, что требует полного понимания и овладения характеристиками вирусов, а также принятия эффективных превентивных мер против них.

В связи с частым возникновением проблем информационной безопасности компьютерных сетей в настоящее время для работы компьютеров применяется все больше антивирусного программного обеспечения, которое играет важную роль в обеспечении безопасности работы компьютерных сетей, предотвращении появления вирусов, спам-сообщений [3]. Поэтому в эпоху больших данных мы должны усилить эффективное применение антивирусного программного обеспечения и системы идентификации электронной почты. Антивирусное программное обеспечение может быть объединено с технологией брандмауэра. Антивирусное программное обеспечение может эффективно выявлять вирусы и злокачественное программное обеспечение, перехваченное межсетевым экраном, а затем проводить эффективное блокирование вирусов.

Система идентификации почты - это в основном система защиты от спама. В настоящее время многие вирусы и вредоносные программы проникают в компьютер через почту. Система идентификации почты будет идентифицировать почту. Если в процессе идентификации почты есть конфиденциальная информация, система автоматически очистит ее. Применение антивирусного программного обеспечения и системы идентификации позволяет эффективно обеспечить стабильность и безопасность работы системы.

Цифровая подпись (ЦП) - это метод аутентификации цифровой информации, основанный на технологии шифрования с открытым ключом. ЦП может эффективно гарантировать безопасность сетевой информации и электронной почты. Кроме того, ЦП возможно идентифицировать и проверять электронные документы, тем самым эффективно обеспечивая конфиденциальность и целостность электронной почты.

Шифрование файлов относится к шифрованию сетевой информации и данных с целью предотвращения их кражи, чтобы способствовать улучшению конфиденциальности. В настоящее время широко используемая технология шифрования файлов компьютерной сети имеет два вида функций: шифрование файлов и коммерческое программное обеспечение для шифрования [4]. Коммерческое программное обеспечение шифрования, в основном, реализуется алгоритмом шифрования. Например, существуют специализированные программные обеспечения для шифрования папок. Также необходимо отметить, что при шифровании файлов лучше дополнительно создавать резервные копии и хранить их в другом месте.

Исследования о том, как лучше защитить безопасность компьютерных сетей, играют важную роль в защите информационной безопасности и интересов пользователей сети. Поскольку компьютерная сеть может быть атакована вирусами, атаками по электронной почте, открытой сетью и произвольной загрузкой прикладного программного обеспечения, хакерским вторжением. Компьютерная сеть нуждается в усилении управления учетными записями, «защитными стенами», антивирусными программными обеспечениями, системой идентификации электронной почты и цифровой подписи.

1. Соловьев А. А., Метелев С. Е., Федоров А. Э. Защита информации и информационная безопасность. - Омск, 2011.
2. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Учебное пособие / НИУ ИТМО. СПб., 2012.

3. Щербакова А.Ю. Алгоритм обнаружения и анализа инцидентов информационной безопасности на основании их факторов // Открытые инновации – вклад молодежи в развитие региона: сб. матер. рег. молодежного форума (г. Пенза, 6 декабря 2013 г.). – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 225–226.
4. Щербакова А.Ю. Вероятностная оценка последствий инцидентов информационной безопасности // Труды междунар. симпозиума «Надежность и качество – 2013». – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 125–128.

Асейдулин И.Р.

Исследование низкоэнергетической адаптивной кластеризации на основе иерархической маршрутизации беспроводных сенсорных сетей

*Самарский государственный технический университет
(Россия, Самара)*

doi: 10.18411/lj-07-2020-63

idsp: ljjournal-07-2020-63

Аннотация

Технология маршрутизации является одной из основных вспомогательных технологий беспроводных сенсорных сетей. Только разумно используя алгоритм маршрутизации или находя лучший алгоритм оптимизации маршрутизации, можно максимизировать функцию беспроводных сенсорных сетей. Поэтому исследование технологии маршрутизации для беспроводных сенсорных сетей имеет важное теоретическое и практическое значение. Основываясь на анализе существующих протоколов маршрутизации в беспроводных сенсорных сетях, в данной статье основное внимание уделяется низкоэнергетическому адаптивному протоколу иерархии кластеризации.

Ключевые слова: кластеризация, беспроводные сенсорные сети, гетерогенные сенсорные сети, алгоритм оптимизации.

Abstract

Routing technology is one of the main auxiliary technologies of wireless sensor networks. Only by intelligently using the routing algorithm or finding the best routing optimization algorithm can the function of wireless sensor networks be maximized. Therefore, the study of routing technology for wireless sensor networks is of great theoretical and practical importance. Based on the analysis of existing routing protocols in wireless sensor networks, this article focuses on the low-energy adaptive clustering hierarchy Protocol.

Keywords: clustering, wireless sensor networks, heterogeneous sensor networks, optimization algorithm

Беспроводные сенсорные сети (WSNs) были широко применены для исследования поля боя, реабилитационной терапии и мониторинга полевой среды. В вышеупомянутой прикладной среде развернуты многочисленные чувствительные узлы. Чувствительные узлы могут воспринимать данные об окружающей среде в режиме реального времени, а затем передавать их в центр управления данными для осуществления мониторинга окружающей среды. Однако из-за ограниченности энергии, подаваемой чувствительными узлами, энергопотребление этих узлов является ключевым фактором, влияющим на эффективность сбора данных WSNs и сокращающим срок службы сети. Как только у узлов заканчивается энергия, они не могут воспринимать данные окружающей среды, что создает лазейки в покрытии WSNs и сокращает его срок службы. Следовательно, целью исследования является повышение использования энергии WSN.

Протокол низкоэнергетической адаптивной кластерной иерархии (LEACH) генерирует вершины кластеров случайным образом и учитывает остаточную энергию