января 2010 года компанией Apple интернет-планшет iPad с размером экрана 9,7 дюйма, во многом являющийся эволюцией карманного компьютера.

Таким образом, интернет-планшет очень удобен и используются для следующих видов работ:

1) Просмотра различных веб-сайтов и веб-страниц;
2) Запуска всевозможных веб-приложений;
3) Чтение электронных книг;
4) Работы с какими–либо веб-службами;
5) Просмотра фотоальбомов, видео- и аудио-файлов;
6) Работы с электронной почтой и др.

Литература

Свободная общедоступная мультиязычная универсальная интернет-энциклопедия [Электронный ресурс]. Режим доступа: http://www.wikipedia.org/. Дата доступа: 25.03.2012.

Макатович Н.С

БГЭУ, ИСГО, группа 11 ДИМ-1, 1 курс

СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В 21 веке наблюдается активный процесс создания информационного общества. Так как возростает важность информации, то и увеличивается и число неправомерных попыток доступа к ней. В связи с этим, возникает логичный вопрос, а как тогда защитить информацию от несанкционированного доступа и использования?

Цель моей работы – рассмотреть основные способы обеспечения информационной безопасности, дать им характеристику, определить недостатки и преимущества.

Угроза — одно из ключевых понятий в сфере обеспечения информационной безопасности. Необходимо выделить два наиболее важных типа угроз: 1) намерение нанести вред, которое появляется в виде объявленного

мотива деятельности субъекта; 2) возможность нанесения вреда – существование достаточных для этого условий и факторов.

Обеспечение информационной безопасности достигается системой мер, направленных: на предупреждение угроз; на выявление угроз; на обнаружение угроз; на локализацию преступных действий; на ликвидацию последствий угроз.

Все эти мероприятия используются для защиты информационных ресурсов от противоправных действий и обеспечения:

- предотвращения разглашения и утечки конфиденциальной информации;
- запрещения несанкционированного доступа к конфиденциальной информации;
- сохранение целостности, полноты и доступности информации;
- обеспечение авторских прав.

Защита от несанкционированного доступа к конфиденциальной информации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации.

На практике все мероприятия по использованию технических средств защиты информации можно поделить на три группы: организационные; организационно-технические; технические.

Технические мероприятия – это мероприятия, которые обеспечивают приобретение, установку и использование специальных, защищенных от побочных излучений средств.

Защитные действия, способы и мероприятия по обеспечению информационной безопасности можно классифицировать по основным характеристикам и объектам защиты по таким параметрам, как характер угроз, направления, масштаб, способы действий и другие.

На данный момент существует большой выбор способов защиты информации, которые имеют свои преимущества и недостатки. Наиболее эффективным будет применение совокупности мер по защите информации.

Кроме того, в большей степени следует уделить внимание мерам по предупреждению несанкционированного доступа, так как легче предупредить, чем ликвидировать последствия.

Литература

1. Википедия Свободная энциклопедия [Электронный ресурс] - 2012. - Режим доступа: http://ru.wikipedia.org/wiki/- Дата доступа: 11.04.2012.

2. Методическая копилка учителя информатики [Электронный ресурс] - 2012.- Режим доступа: http://www.metod-kopilka.ru/page-2-2-3.html./-Дата доступа: 11.04.2012.

3. Asher's Attic [Электронный ресурс] - 2012.- Режим доступа: http://asher.ru/security/book/shsh/05.- Дата доступа: 11.04.2012

Маргунов Е.А.

ГГТУ, ФАИС, группа ЗМаг-11, магистрант

СРАВНЕНИЕ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРОМ И МЭЙНФРЕЙМОМ ЧЕРЕЗ ПРОТОКОЛЫ FTP И TN3270

В связи с необходимостью передачи больших объемов данных между различными платформами в крупных масштабируемых системах, встает проблема обеспечения максимальной пропускной способности канала для поддержки высоких вычислительных возможностей больших серверов класса мэйнфрейм.

Целью данного исследования является сравнение скорости передачи данных между операционными системами семейства Windows (персональный компьютер) и операционной системой z/OS (мэйнфрейм) посредством протоколов FTP и TN3270. Для достижения поставленной цели спроектирован и разработан визуальный FTP клиент, позволяющий передавать данные между указанными платформами. Протокол TN3270 является диалектом протокола telnet, используемого для реализации терминального доступа к различным