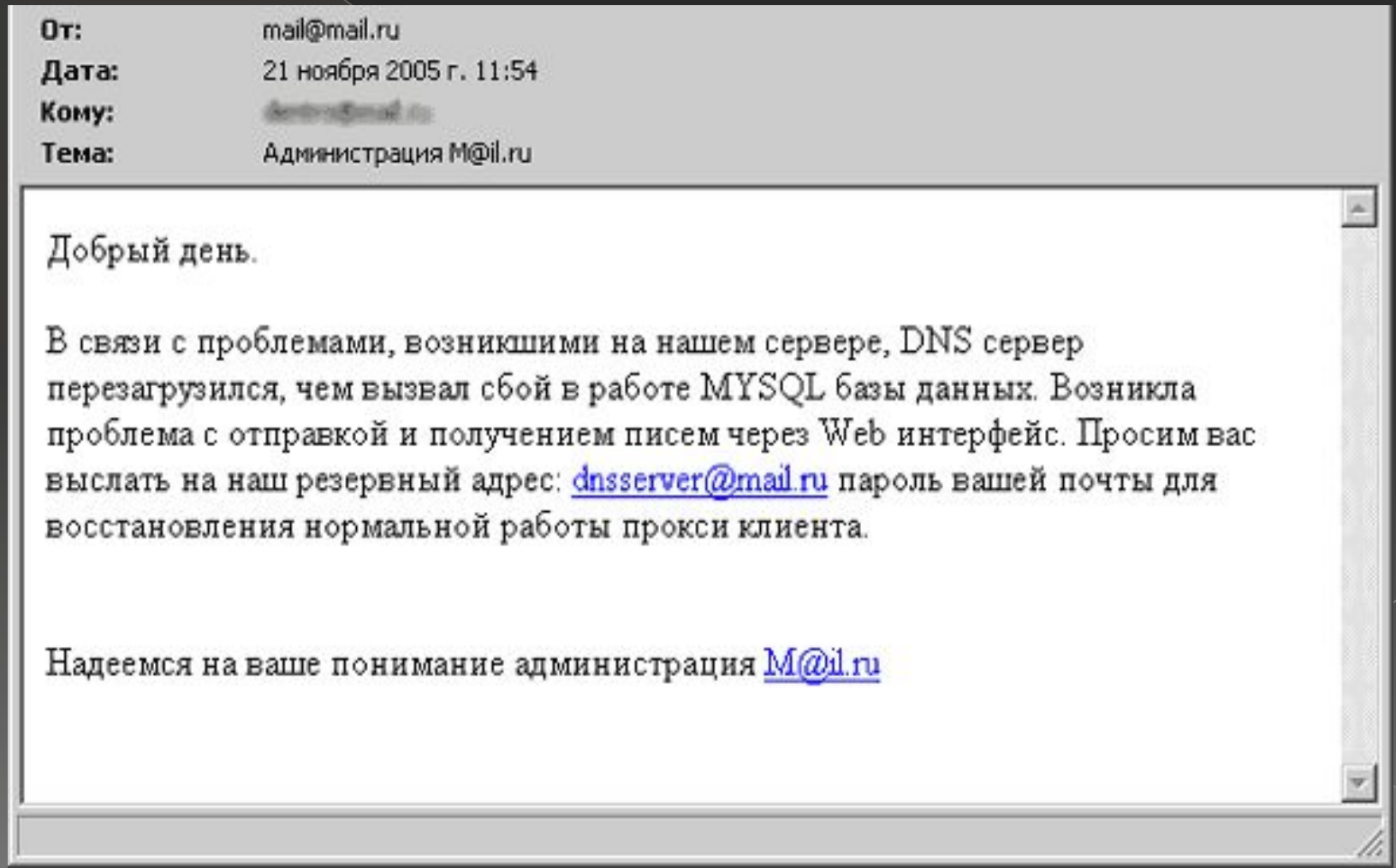
# Хакерские атаки и взломы телекоммуникационных систем.

Хакеры проникают в компьютеры так же, как воры - в дома и квартиры. Вы знаете, как именно это происходит и как защититься от незаконного вторжения?

- **Fishing (или Фишинг).** Очень широкое понятие. Смысл его в том, чтобы получить от пользователей информацию (пароли, номера кредитных карт и т.п.) или деньги. Этот приём направлен не на одного пользователя, а на многих.



**От:** mail@mail.ru
**Дата:** 21 ноября 2005 г. 11:54
**Кому:** [redacted]
**Тема:** Администрация M@il.ru

Добрый день.

В связи с проблемами, возникшими на нашем сервере, DNS сервер перезагрузился, чем вызвал сбой в работе MYSQL базы данных. Возникла проблема с отправкой и получением писем через Web интерфейс. Просим вас выслать на наш резервный адрес: dnsserver@mail.ru пароль вашей почты для восстановления нормальной работы прокси клиента.

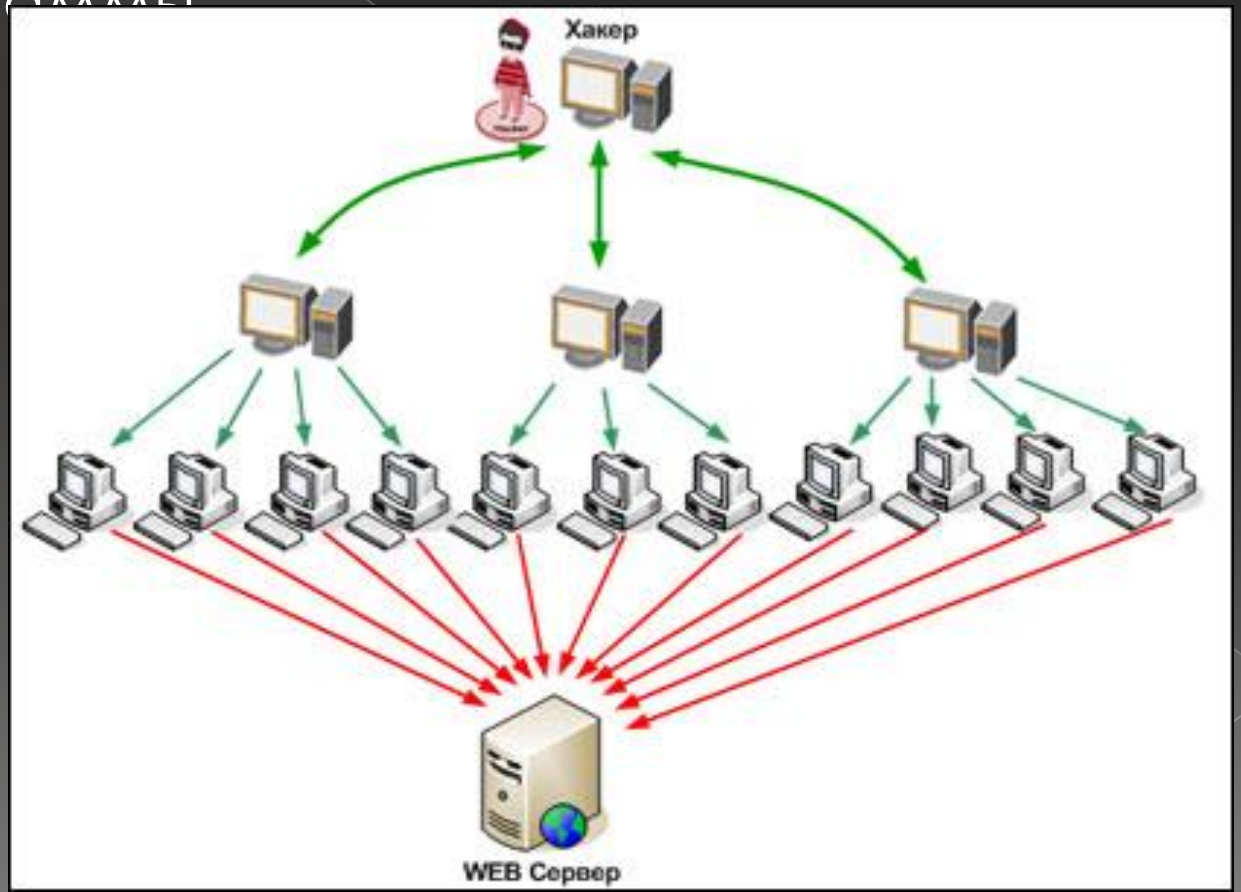
Надеемся на ваше понимание администрация M@il.ru

- **Социальная инженерия** – это не технический, а психологический приём. Пользуясь данными, полученными при инвентаризации, взломщик может позвонить какому-либо пользователю (например, корпоративной сети) от имени администратора и попытаться узнать у него, например, пароль. Это становится возможным, когда в больших сетях, пользователи не знают всех работников, и тем более не всегда могут точно узнать их по телефону. Кроме этого, используются сложные психологические приёмы, поэтому шанс на успех сильно возрастает.
- Рекомендации: те же самые. Если действительно есть необходимость, то сообщите нужные данные лично. В том случае, если Вы записали пароль на бумаге, не оставляйте её где попало и по возможности уничтожайте, а не просто выбрасывайте в мусорную корзину.

- **Вирусы.** Самая известная простому пользователю проблема. Суть во внедрении вредоносной программы в компьютер пользователя. Последствия могут быть различны и зависят от вида вируса, которым заражён компьютер. Но в целом - от похищения информации до рассылки спама, организации DDoS атак, а так же получения полного контроля над компьютером.

| | |
|---|---|
| **Файловые** | Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОП до выключения компьютера |
| **Загрузочные** | Записывают себя в загрузочный сектор диска (в программу — загрузчик ОС). При загрузке ОС с зараженного диска внедряется в ОП и ведет себя как файловый вирус |
| **Макровирусы** | Являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОП до закрытия приложения |
| **Драйверные** | Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки |
| **Сетевые** | Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам |

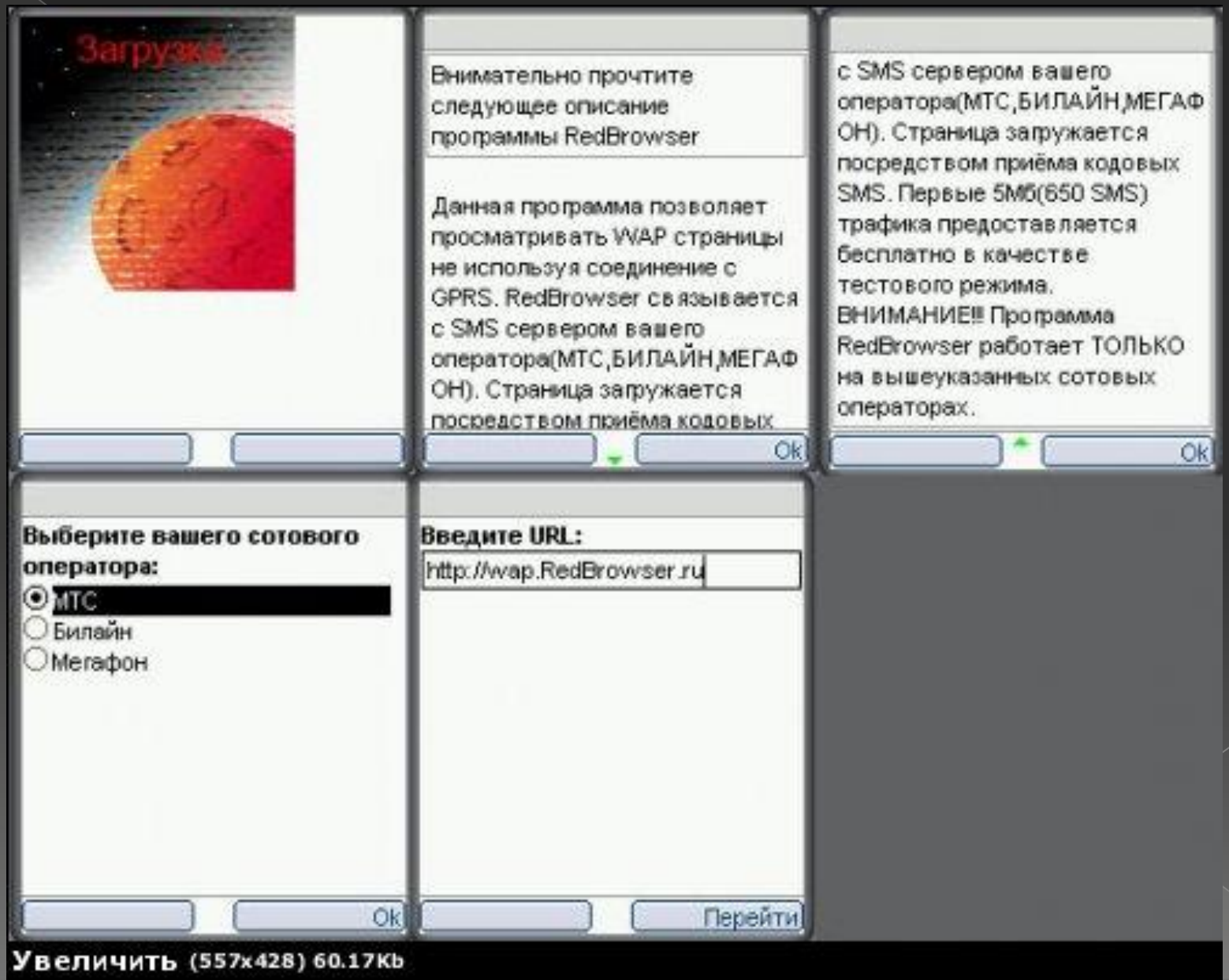
- **DoS (Denial of Service или Отказ от Обслуживания).** Это скорее не отдельная атака, а результат атаки; используется для вывода системы или отдельных программ из строя. Для этого взломщик особым образом формирует запрос к какой-либо программе, после чего она перестаёт функционировать. Требуется перезарузка, чтобы вернуть рабочее состояние програ[illegible]



# DoS-атаки против ряда сотовых телефонов при помощи множественных посылок файлов с использование ПО ussp-push.

При использовании атаки телефон жертвы начинает выдавать множество сообщений, требующих получить, либо отвергнуть передаваемые файлы. Так как скорость передачи достаточно высока, через определённое время телефон попросту зависает, не давая, в том числе, отключить Bluetooth.

# Вирусы сотовых телефонов



# Стратегия обороны

Стратегия защиты мобильного телефона и смартфона от вирусной атаки довольно проста. За редким исключением, вредоносные приложения не активизируются сами по себе. Как правило, их включает введенный в заблуждение владелец телефона. Поэтому первое и главное правило гласит: не скачивайте приложения, в которых вы не уверены, не открывайте подозрительные MMS-сообщения со ссылками.

Между прочим, наделавший столько бед российским операторам мобильной связи и их клиентам вирус RedBrowser начинал распространяться только тогда, когда его скачивали и разрешали ему рассылать SMS-сообщения. Чуть больше осторожности - и угрозу можно было бы отвести. Не проявляйте ненужного легкомыслия и тогда, когда кто-то, вам не известный, запрашивает соединение. Перед установкой даже вирус вынужден получить на это ваше согласие. Не давайте его.

# Спасибо за внимание!