Полицейские и воры

Свежеслитая база должна быть на рынке завтра!

Чужие секреты — ходовой товар

Первые покупатели не заставили себя долго ждать

На самом деле секьюрити не дремлет

Закономерный финал: продавец схвачен и обездвижен





И так будет с каждым, кто посмеет покуситься на конфиденциальную информацию. Наказание неотвратимо!

Продолжение следует…

Конфиденциальность данных

Информация в России отличается от полезных ископаемых тем, что ее значительно легче добывать. Английский термин «Privacy» можно примерно перевести как «неприкосновенность частной жизни и принцип неразглашения информации личного характера». Полный и исчерпывающий перевод этого всеобъемлющего термина в российских словарях отсутствует.

В течение более 70 лет граждан России усердно и последовательно приучали к приоритету общественных интересов над личными, к ценности коллектива и малозначительности его отдельных «винтиков». Часто звучавшая на собраниях фраза: «Мне нечего скрывать от коллектива!» произносилось с гордостью и чувством глубокого удовлетворения. Возможно, именно с этим своеобразным наследием прошлого и связаны трудности перестройки нашей психологии. Изменить сознание миллионов людей — не денежную реформу провести, времени и усилий требуется куда больше. Проникновение современных технологий во все сферы нашей жизни происходит высокими темпами и порождает новые проблемы в части обеспечения сохранности информации о гражданах.

Криминальная торговля процветает на глазах у милиции

Проблема утечки личной и конфиденциальной информации из государственных и коммерческих структур существу- »

» ет везде, однако в большинстве стран с этим явлением научились эффективно бороться. Подтверждение тому — периодически вспыхивающие громкие скандалы и судебные иски на миллионы долларов.

Что касается России, то у нас воровство и незаконное распространение разнообразных баз данных уже принимает масштабы национального бедствия. Технологии обработки значительных массивов данных совершенствуются, все больше информации оцифровывается и структурируется, все больше сведений о нас с вами переносится с допотопных бумажных карточек в память современных компьютеров. Базы данных растут и объединяются, работать с ними становится все проще и удобнее, к сожалению, не только тем, для кого они создаются.

В отсутствие реально работающих механизмов пресечения воровства масштабы распространения нелегально добытой информации будут прямо пропорциональны общим темпам компьютеризации государственных и коммерческих структур. Оценить масштабы воровства несложно — достаточно поинтересоваться о наличии «специфического товара» у продавца компьютерных дисков. В большинстве случаев вам предложат прямо на месте или пообещают «достать» чуть ли не любую информацию из категории «для служебного пользования». CD-диски с конфиденциальной информацией рекламируют в Интернете и практически в открытую предлагают приобрести в массовых рассылках электронной почты.

Все это безобразие происходит при очевидном попустительстве правоохранительных органов: многие продавцы не стесняются выкладывать «криминальные» диски прямо на свои лотки, явно не опасаясь ни гражданской, ни уголовной ответственности. И это притом, что сам факт наличия у продавца диска с информацией типа «Оперативная база данных по лицам, находящимся в федеральном розыске» автоматически подразумевает целый букет нарушений закона! Продавца можно (и нужно) привлекать к ответственности прямо на месте, никаких хитроумных экспертиз (как с пиратскими видеокассетами) не требуется. Однако это почти никогда не делается. Почему?

Просто справочная информация?

Известный аргумент: «Продается открытая информация справочного характера». Этакие добрые дяди, готовые за стодвести рублей снабдить вас полным архивом «Мосгорсправки» вместе со всей информацией, предоставляемой справочной службой «09». В какой-то мере справедливо. Действительно, в России существует дефицит грамотно сделанных и хорошо структурированных электронных справочников, а некоторые виды библиотек отраслевых нормативных документов можно приобрести только в пиратском исполнении.

Можно дискутировать на тему того, является ли криминальной база данных с телефонами, адресами и фамилиями всех абонентов городской телефонной сети — в других странах фолиант с такой информацией лежит в каждой телефонной будке. Правда, что-то я не приметил в таких справочниках полных домашних адресов, да и размещение в нем информации — дело сугубо добровольное.

Но речь о совсем другой «справочной информации». Свободно продаются полные базы данных поставленных на учет транспортных средств (номер автомашины, фамилия и паспортные данные владельца, номера двигателя и кузова и т. п.), система оперативного поиска информации «Розыск-судимость», подробная база данных по всем московским квартирам (с характеристиками жилья, адресами и паспортными данными владельцев) и многое другое.

Последний по времени скандал — появление в свободной продаже базы данных сотовой сети МТС с подробной информацией о клиентах: ФИО абонента, номер мобильного и домашнего или рабочего телефона, паспортные данные, дата рождения, адрес местожительства, банковские реквизиты оплачивающей »

По сходной цене

Продается все

Некоторое начальное представление об этом процветающем бизнесе можно получить из многочисленных «рекламных» рассылок, однако оценить его истинные масштабы позволяет только прямое общение с продавцами. Ниже — неотредактированная часть переписки с одним из поставщиков «конфиденциального контента»:

«Я очень сильно извиняюсь :((но произошло то, что мой брат по ошибке увез не тот диск. Увез к себе домой именно МТС базу:((сегодня ее забрать уже никак не получается...

есть вариант:

мы сегодня встречаемся и я Вам передаю 5 баз = итого 500 рублей... и еще если интересуют:

1 — «БАЗА ДАННЫХ ПО АДМИНИСТРАТИВНЫМ ПРАВОНАРУШЕНИЯМ»

2 — «БАЗА ДАННЫХ ПО ДОРОЖНО-ТРАНСПОРТНЫМ ПРАВОНАРУШЕНИЯМ»

3 — «ФЕДЕРАЛЬНЫЙ РОЗЫСК»

4 — «Должники ГНИ»

5 — Телефонный справочник ведомств и крупнейших предприятий РФ

6 — «База данных по изъятым записным книжкам — 2000»

7 — БД «Похищенные паспорта»

8 — БД «ЛАБИРИНТ-2000». Август 2002 года. База данных досье на политиков, предпринимателей, государственные органы, коммерческие структуры и многое другое. Имеется встроенный рубрикатор и гипертекстовая структура. Данные на август 2002 г.

9 — База данных по преступным группировкам

10 — Система оперативного поиска информации «Розыск-судимость»

11 — ЧОПы

все эти 11 баз за...500 рублей... + те 5, итого 1000 р. Завтра-послезавтра я заберу МТС у брата и отдам ее ...сделаю скидку.....за 1000 рублей! Идет?

Комментарии, как говорится, излишни. Остается только пожалеть бедного продавца-сироту: учитывая всеобъемлющий характер предлагаемых к продаже «ресурсов», его родители тоже наверняка присутствовали бы в одной из баз. А подозревать человека в продаже за три копейки всех сведений о собственной маме не хочется — как-то уж совсем некрасиво, не знаю, как помягче охарактеризовать такое деяние...

Мошенничество

Легальный бизнес «по-русски»

Последняя криминальная история с пропажей и торговлей свежей базой данных неожиданно дала толчок целому новому направлению в этом бизнесе. Технология проста до смешного: в архив RAR закатывается своп-файл собственного компьютера, архив закрывается паролем. Затем безобидный файл сливается на болванку CD-R и продается за 200 рублей под видом «наисвежайшей базы данных». Пикантность ситуации в том, что продавец такого товара практически ничем не рискует. Не пойдет же покупатель жаловаться в милицию на то, что ему всучили «куклу» вместо обещанной, например, базы данных со списком телефонов всех сотрудников УВД.

Для оперативного уточнения адреса квартиры и фамилии ее владельца достаточно набрать в строке поиска номер квартирного телефона Москвы или Питера. Для справки: 90% продаваемых сегодня мобильников имеют встроенный WAP-браузер. Цена получения запрошенной информации — 17 с эфирного времени, или 3,5 Кбайт переданных по каналам GPRS данных.

Очередной массовый тираж базы данных квартирных телефонов. В этом продукте уже реализована система сквозного поиска телефонных номеров/адресов по нескольким городам России. Информация не самая свежая, а под «сотовыми телефонами» подразумеваются абоненты систем «Искра» и «Алтай». Но и цена соответствующая — 60 рублей «в базарный день». На коробке издевательская надпись: «Информация предоставлена спецотделом ГосКомСвязьНадзора России».

» телефон организации и т. д. Удобная система поиска позволяет, например, за несколько секунд получить полный список «мобилизированных» сотрудников того или иного предприятия с их паспортными данными, домашними адресами и т. п.

Кстати, появившиеся об этом заметки в разных средствах массовой информации (газета «Ведомости» от 21 января 2003 года и другие издания) заставляют предположить кражу не только абонентской базы данных, но и части основной биллинговой системы, так как корреспонденты «Ведомостей» пишут об информации о «прошедших платежах», которые в абонентской базе данных обычно не фиксируются.

Нелегальный мобильный справочник

В прессе регулярно появляются сожаления о недостаточной популярности мобильного Интернета (WAP-ресурсов). Зря сожалеют: «специфической» информации там более чем достаточно, и наверняка ей пользуются — а иначе зачем ее там размещать? Например, на нескольких WAP-сайтах широко доступны все данные о владельцах квартирных телефонов Москвы и Санкт-Петербурга, причем с возможностью поиска как по номеру телефона, так и по адресу владельца. Видимо, размещение в мобильном Интернете базы данных ГИБДД с именами, адресами и телефонами автовладельцев — дело недалекого будущего. Надо ведь облагодетельствовать не только квартирных воров, но и угонщиков автомобилей, правда?

Вопрос поставлен — ответа нет

Печально, но в большинстве случаев отследить путь утечки информации не удается. Что означает безнаказанность виновных и, соответственно, предпосылки к повторению подобных случаев в будущем.

Хотя до случая с МТС таких масштабных «уводов» информации об абонентах (миллионы единиц) сотовых сетей не происходило. Комментирует Ева Прокофьева, пресс-секретарь МТС: «Недавно нам стал известен факт утечки некоторой части базы данных МТС — номера телефонов наших абонентов. Специалисты службы МТС, занимающейся защитой информации, провели расследование. Выявить конкретный источник утечки, опираясь на формат данных, не удалось. Дело в том, что существует целый ряд законодательных актов (Закон РФ о связи, Постановление правительства №30 (15.01.93), особые условия лицензий на предоставление услуг сотовой радиотелефонной связи), а также нормативных документов, выпущенных регулирующими и силовыми ведомствами, в соответствии с которыми все операторы обязаны предоставлять им информацию в согласованном порядке. В результате увеличивается вероятность появления разных источников утечки информации. Для пресечения подобных утечек в компании приняты самые серьезные меры. Доступ к базе данных МТС строго регламентируется, а сама база защищена от несанкционированных действий».

Вне зависимости от места работы виновника и способа кражи вывод из происшедшего очевиден: государство в лице правоохранительных органов хочет иметь (и имеет!) полный доступ ко всей информации о своих гражданах, но при этом практически ничего не предпринимает для обеспечения защиты такой информации.

Под защитой в данном случае следует понимать не только заботу государства о сохранности собственной конфиденциальной информации, но и эффективно работающие механизмы предотвращения увода такой информации из коммерческих структур.

Другая сторона медали

В постперестроечные годы стало модно сваливать собственные ошибки и безалаберность на происки спецслужб. Необходимость предоставления «компетентным органам» доступа к информации вполне может служить удобным оправданием для оператора связи. У семи нянек дитя без глазу, а коллективная ответственность слишком часто оборачивается отсутствием таковой вообще.

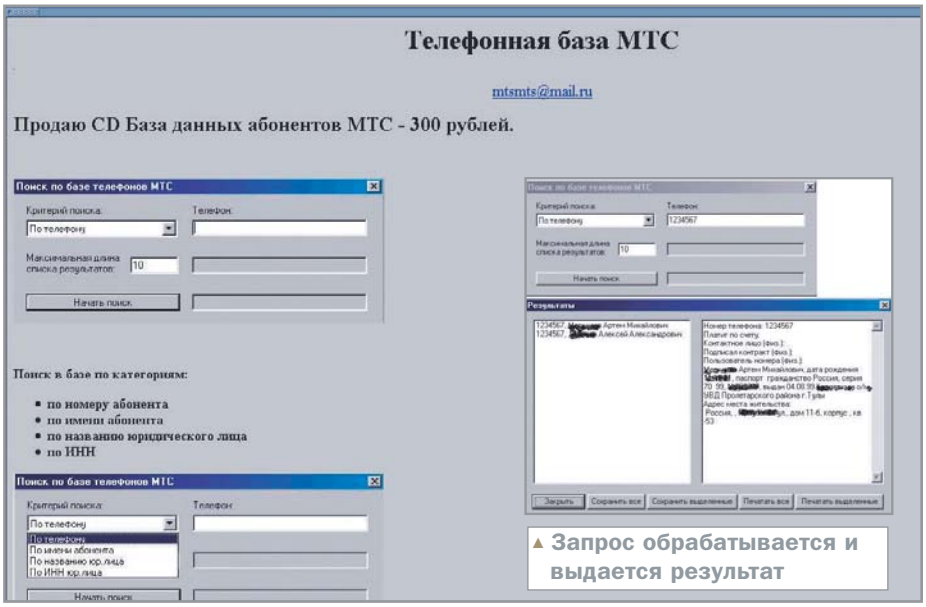
Что касается абонентских баз операторов, то настораживает факт «необъяснимой» пропажи только базы данных абонентов МТС. Руководство «Билайн» высказывается на эту тему достаточно ос- »

» торожно, что вполне объяснимо: не так давно многие «активные» (то есть выгодные для компании) абоненты «Билайн» получили от руководства МТС персональные электронные письма с предложением сменить оператора — как-то удалось добыть список таких абонентов!

Руководители «МегаФона», МСС и «Сонета» заявили о невозможности подобных инцидентов у себя, что как минимум свидетельствует об их уверенности в возможности предотвратить такие инциденты собственными силами. Хочется верить, что происшедшее послужит серьезным предупреждением для всех операторов. В том числе и для руководства МГТС, чьи «обновленные» версии абонентской базы появляются на рынке чуть ли не чаще очередных релизов программных продуктов Microsoft. Увы, пока поводов для оптимизма нет: в начале февраля в Новосибирске было заведено уголовное дело на сотрудника местного филиала сети МТС — менеджер в свободное время приторговывал детализациями (расшифровками данных) телефонных переговоров предпринимателей Новосибирского региона.

Каких сюрпризов ждать от новых технологий

Многие гигабайты информации «для служебного пользования» уже лежат в обоих сегментах Рунета — обычного и мобильного (WAP). Ситуация начинает напоминать театр абсурда: «специально обученные» сотрудники коммерческих фирм буквально через мелкое сито ежедневно просеивают интернет-контент — не дай бог, кто-нибудь выложит фотографию модели до официального начала продаж. И у них это очень неплохо получается. Выходит, могут если захотят?



▲ Искать можно практически по любому полю в базе. Это свидетельство и полноты базы, и умения специалистов «предпродажной подготовки»

У государственных органов возможностей ничуть не меньше, а рычаги давления на хозяев интернет-ресурсов намного более серьезные. Однако действия по блокированию сайтов с информацией личного характера незаметны. Технологии не стоят на месте и в условиях молчаливого попустительства такая «открытость» ни к чему хорошему не приведет. Общая тенденция — повышение скорости доступа к сетевыми ресурсам и тарификация не по времени пребывания в Сети, а по объему потребленной информации. Плюс к этому — постоянное подключение к Сети терминала, будь это компьютер в офисе, КПК или смартфон. Для ПК это локальные сети с каналом подключения к Интернету, ADSL-подключение по телефонной линии и т. п.; для мобильного терминала — подключение по каналу GPRS, радиосеть WLAN и т. п.

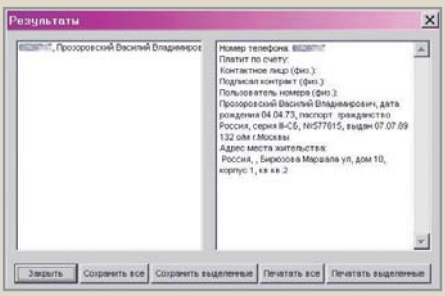
С развертыванием сетей третьего поколения и ростом скорости нетрудно представить картину любого уровня мрачности. Например, в мобильных сетях это может быть определение номера звонящего с мгновенным автоматическим опросом доступных баз и выводом на дисплей «всей подноготной»: ФИО, паспортных данных, номера автомобиля, адреса, места работы и краткой выписки из карточки истории болезни в поликлинике. ■ ■ ■ **Сергей Потресов**

Ответ ворам

Не все потеряно

Конечно же, крайне неприятно получать в подарок от коллег скриншот со своими личными данными. Это всего лишь шутка, но как могут использовать эти данные злоумышленники, особенно против обеспеченных людей, даже думать не хочется.

Однако не все потеряно. Практически сразу после того, как стало известно о факте похищения, начальник управления внешних связей холдинга «Система Телеком», крупнейшего акционера МТС, Виктор Исаев, сообщил, что МТС располагает необходимыми ресурсами для бесплатной замены телефонных номеров своим абонентам в связи с нарушением конфиденциальности информации о них в базе оператора. Оценивая возможные последствия раскрытия информации об абонентах МТС, компания не ожидает слишком активной смены номеров. Но, как показала практика, слова главного акционера — это одно, а проза жизни — совсем другое. На сайте МТС нет никакого упоминания о факте утечки, что понятно, и никакой информации о том, как можно поменять номер. Следовательно, узнать об этом механизме можно будет лишь в справочной, а сама процедура будет затянута и затруднена.

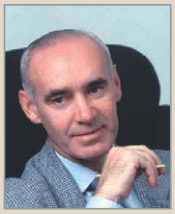


Прямая речь

Александр Маношкин, ведущий специалист по рекламе и связям с общественностью ОАО «Московская сотовая связь»

Утечек информации о клиентах не происходило. «Компетентные» органы могут получить доступ к базе данных компании, содержащей информацию об абонентах, только по постановлению соответствующего судебного органа.

С сотрудниками компании заключается контракт, включающий в себя специальное положение о неразглашении конфиденциальной информации. Информационная система компании защищена от возможных атак хакеров извне современными программными средствами, а каждый сотрудник в соответствии с исполняемыми обязанностями получает определенный соответствующий уровень доступа к базе данных. ■ ■ ■



Владимир Морозюк, генеральный директор компании «Персональные коммуникации» (сотовая сеть «Сонет»)

За время существования компании случаев появления в открытом доступе абонентской базы нашей компании не было зафиксировано.

Сотрудники у нас имеют доступ не ко всей базе данных одновременно, а к отдельному абоненту. Думаю, что так у всех операторов. ■ ■ ■

Роман Проколов, руководитель PR-отдела ЗАО «СоникДуо» (торговая марка «Мегафон»)

Нет, в московской сети «МегаФон» таких утечек не было. Нами приняты серьезные меры по защите информации о московских абонентах.

В соответствии с действующим законодательством правоохранительные органы имеют право на получение информации о клиентах коммерческих фирм — на основании соответствующих судебных решений. То есть прямого доступа к базе данных у органов нет — оператор сам предоставляет им информацию по теме официального письменного запроса.

Все базы данных компании надежно защищены от несанкционированного доступа с помощью самых современных технических решений, а доступ к информации об абонентах «МегаФона» строго ограничен кругом соответствующих специалистов — и даже внутри этой группы есть разные уровни доступа. Все обращения к базе данных фиксируются и контролируются. Есть и еще ряд средств защиты, которые не могут быть разглашены. ■ ■ ■

Михаил Умаров, директор по связям с общественностью «Билайн»

Вопросы обеспечения конфиденциальности личной информации абонентов являются составной частью системы информационной безопасности компании. Руководство «Вымпелкома» ставит задачу обеспечения адекватного уровня защиты, соответствующего мировым стандартам в телекоммуникационной отрасли.

К сожалению, мы имеем негативный опыт, когда несколько лет назад произошла утечка части информации об абонентской базе. Правда, тогда компания работала в стандарте DAMPS и обслуживала около 100 000 клиентов. Было проведено внутреннее расследование, выявлен нарушитель, приняты меры в соответствии с действующим законодательством.

Так, одним из значимых шагов в повышении уровня безопасности данных явилась реализация проекта замены биллинговой системы. Но вопрос безопасности не может быть закрыт — это процесс, требующий постоянного внимания.

Однако следует признать, что для обеспечения работы доступ к личной информации абонентов предоставляется большому количеству внутренних пользователей (сотрудники службы поддержки и администраторы систем), некоторым организациям, а также компетентным органам.

Поэтому вопросы безопасности, связанные с человеческим фактором, имеют первостепенное значение, и риск, связанный с этим аспектом, остается высоким.

Да, были найдены виновные и сделаны выводы из ситуации, в том числе по укреплению внутренней системы безопасности.

Мы принимаем самые серьезные меры, чтобы подобная информация не попала к тому, к кому она не должна попасть. ■ ■ ■

Ева Прокофьева, пресс-секретарь МТС

К сожалению, приходится констатировать, что утечки информации из баз данных организаций происходят регулярно, и это уже вышло из разряда неординарных событий. Достаточно вспомнить нашумевшую историю с продажей практически всей базы данных по автовладельцам. Более мелкие утечки выявляются чуть ли ни каждый день. Не минует эта беда и операторов.

И сегодня на рынке продается CD неизвестного происхождения, выдаваемый за базу данных абонентов МТС московского региона. Продаваемая продукция является компиляцией достоверных и недостоверных данных о физических и юридических лицах, в разное время бывших абонентами МТС в Московском регионе.

В настоящее время компания проводит внутреннее расследование, которое еще не завершено. Пока назвать виновных нельзя. В то же время мы обратились в компетентные органы для поиска заказчиков, изготовителей скомпилированной базы данных и ее распространителей.

Для обеспечения невозможности подобных утечек в компании приняты самые серьезные меры. Доступ к базе данных МТС регламентируется, а сама база защищена от несанкционированных действий. Кроме этого, сейчас мы проводим дополнительную экспертизу своей информационной системы и разрабатываем комплекс технических и организационных мероприятий по защите данных. ■ ■ ■