**А.И. Гладышев**[1]

# УДОБСТВО И БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. В ЧЕМ ПРОТИВОРЕЧИЕ?

*В статье рассматриваются компьютерные технологии, которые в первую очередь тяготеют именно к удобству пользователей, пренебрегая безопасностью. Формулируются задачи в плоскости «удобство – безопасность» на основе методов аутентификации. Применение предложенных подходов позволит существенно повысить безопасность за счет регулирования избыточных удобств пользователей.*

***Ключевые слова:*** *безопасность компьютерных систем, макровирус.*

**A.I. Gladyshev**

## THE CONVENIENCE AND SAFETY OF COMPUTER SYSTEMS. WHAT IS THE CONTRADICTION?

*The article considers computer technologies which gravitate first of all to convenience of users, neglecting safety. Some tasks in the convenience safety plane on the basis of authentification methods are formulated. Application of the offered approaches will allow to increase essentially safety for the account of regulation of superfluous conveniences of users.*

***Keywords:*** *safety of computer systems, macrovirus.*

Каждый, кто летает самолетами, знаком с довольно хлопотной процедурой предполетного досмотра: очередь к рамке, возня с тазиками для обуви и одежды, выброшенные в корзину маникюрные ножницы, бутылки с минеральной водой и прочие несовместимые с полетом предметы. Весьма неудобно для пассажиров, но таковы требования безопасности.

Это касается безопасности в любой области: хочешь сохранить жизнь в ДТП – не поленись пристегнуться (неудобно), хочешь обезопасить себя от гриппа – ходи в ватно-марлевой повязке (тоже неудобно) и т.д. Должна ли быть исключением информационная безопасность? На нескольких примерах мы посмотрим, как компьютерные технологии, которые в первую очередь тяготеют именно к удобству пользователей, постоянно заставляют его расплачиваться безопасностью.

Одна из сложно решаемых задач в плоскости «удобство–безопасность» – это аутентификация. Именно аутентификация – процедура надежного опознавания пользователя (в более широком смысле также устройств, программ) – ключевой механизм системы безопасности. Методов аутентификации пользователей, по сути, всего три, ничего другого пока не придумано: по паролю (секретной последовательности, известной только пользователю), по физическому носителю (собственно по тому же паролю, только записанному на смарт-карту, USB-устройство и т.д.) и по биометрическим данным.

Исторически первым и удобным средством аутентификации был пароль. Он же остается главным средством и по сей день. В принципе, при условии, что пароль выбран случайно, из большого алфавита и достаточно длинный, гарантирована невозможность подбора даже с применением мощного компьютера. PIN-кодов из четырех цифр всего 10 тысяч, поэтому в банкоматах и мобильных телефонах ограничивают число попыток ввода. А вот 8-значных паролей типа «цифры+буквы+регистр» (именно такие пароли используются в более-менее защищенных системах) будет уже 218 триллионов.

Но пользователю легче запомнить пароль из имени любимой собаки, чем выданную администратором абракадабру вроде “Khp5dsGY”. Как следствие, использование неслучайных паролей открывает возможность «атаки по словарю», а это сокращает время на подбор пароля в разы, сдвинув его из теоретической области (несколько сотен лет) в область практическую (пару часов).

[1] Кандидат технических наук НОУ ВПО «Российский новый университет».

Вопрос для самоконтроля: что будет, если заставить среднестатистического пользователя использовать случайный длинный пароль? Такая возможность есть у администратора. Правильно, он запишет на листочке и приклеит к монитору – удобно. Более осторожные листочек спрячут под клавиатуру или под мышиный коврик. О безопасности в этом случае говорить неуместно.

От необходимости запоминать пароли избавляют физические носители – магнитные карты, USB-ключи и т.д., но они могут быть утеряны или украдены. Много надежд в свое время возлагалось на биометрию как удобное и безопасное средство аутентификации. Ну действительно, сама природа побеспокоилась, чтобы у каждого из нас был свой уникальный «пароль» на папиллярном рисунке кожи пальцев, на радужной оболочке глаза, в голосе, лице, жестах и походке. Собственно, по биометрическим характеристикам мы друг друга и аутентифицируем.

Настоящий бум на биометрические системы начался после событий 11 сентября 2001 года, когда в США были брошены миллиарды долларов в попытке чисто технологически решить проблему борьбы с терроризмом. С 2005 года желающие въехать в США обязаны иметь в своих визах либо паспортах биометрическую информацию для аутентификации, отголоски той истерии мы ощущаем до сих пор, стоя в очередях за биометрическими загранпаспортами. Тут-то как раз вроде бы ради безопасности пожертвовали удобством. Но вот, например, опыт системы FaceIt, которая была установлена во многих американских аэропортах и должна была опознавать преступников по базе фотографий, показал, что здесь нет ни безопасности (не удалось задержать ни одного преступника), ни удобства (ложными срабатываниями система просто доводила до исступления полицейских). Это касается и других методов биометрической аутентификации. Например, в начале 2002 года японский криптограф Цутомо Мацумото наглядно продемонстрировал, что с помощью суперклея, желатина и формовочного пластика по отпечатку пальца (!) можно изготовить его муляж, «признаваемый» биометрическим сканером. Аналогичные результаты были получены и другими энтузиастами, о чем можно узнать, например в книге Б. Киви «Гигабайты власти» (электронную версию можно найти на lib.rus.ec). Стоит ли удивляться, что бум на биометрию как на панацею сошел на нет, перейдя в фазу практического использования там, где она действительно эффективна.

Мнимые удобства, размноженные в миллионах копий программного обеспечения, – причина появления многих вирусов, которых могло бы не быть, если бы разработчики ПО больше уделяли внимания безопасности, а не занижали своих оценок интеллектуальных способностей пользователей.

Наглядный пример – функция Autoplay, или Autorun, которая появилась в Windows-95. Как только система обнаруживает новый сменный носитель (предполагалось, что это будет только CD-ROM), она пытается найти файл autorun.inf и в случае успеха автоматически выполняет команды, прописанные в этом файле. Задумано это было, кстати, чтобы снизить затраты на звонки пользователей в службу поддержки. Ведь так здорово: пользователь вставляет в компьютер компакт-диск, и, немного пожужжав дисководом, компьютер автоматически запускает программу установки. Не все, видно, пользователи знают, что для установки программы необходимо найти на диске файл setup.exe и запустить его.

В принципе угрозы эта функция не представляла до тех пор, пока дело касалось дисков CD-ROM, на которые, в принципе, ничего нельзя записать. Но стоило распространиться флэшкам и другим запоминающим USB-устройствам, на которые как раз можно записывать информацию, как Autorun-вирусы бодро зашагали по планете. Пик эпидемий пришелся на 2007–2008 годы (то есть «дыра» ждала своего часа 10 лет), когда каждый месяц появлялась сотня новых вирусов, «отъедавших» 20–30% всех вирусных атак. Все повторяется, еще в ДОСовские времена одним из любимых мест обитания вирусов (правда, легко обнаруживаемых) был пакетный файл autoexec.bat. Только когда стало ясно, что лучше пожертвовать мнимым удобством – по умолчанию в Windows Vista эта функция выключена. Пятнадцать лет понадобилось Microsoft, чтобы прийти к выводу: «Автозапуск» должен быть выключен по умолчанию.

Из той же серии и меню «Автозагрузка» (StartUp) – группа программ, которая существует в Windows с незапамятных времен (версии 3.11). Туда можно прописать программы, которые автоматически запускаются вместе со стартом ОС. Кстати, сами пользователи этой возможностью пользуются крайне редко, зато для распространения вирусов и троянских программ – это весьма заманчивое место. Конечно, прописать себя в прямо в «Автозагрузку» решится только вирус-самоубийца. Для умных вирусов есть аналогичная по функции часть реестра Windows, которая как раз труднодоступна для контроля пользователей. Обращаться с редактором regedit способен далеко на каждый пользователь, но есть мас-

са программ, которые позволяют заглянуть в это небезопасное нутро. Установите, например, бесплатную программу отечественного производства Anvir Task Manager и вы удивитесь, какое количество программ запускаются вместе с Windows…

Анализ вирусных эпидемий прошлых лет заставляет в этом свете вспомнить и про макровирусы, доставившие много проблем пользователям. Большинство из них, наверное, даже и не поняли, что они расплачиваются потерянными нервами и временем за удобство, которое несли в себе макрокоманды (макросы), появившиеся еще в ранних версиях редактора Microsoft Word. Конечно, макросы создавались для того, чтобы пользователь мог автоматизировать рутинные операции обработки текстового документа. Для пущего комфорта какие-то макрокоманды можно было заставить выполняться каждый раз при открытии документа.

Результат не заставил себя ждать. Первый макровирус Concept появился в 1996 году, относительно невинный. Спустя три года другой макровирус Melissa с функцией почтового червя стал одним из первых вирусов, ущерб от которого во всем мире превысил 1 млрд долларов. Многовато за удобство, которое к тому же подавляющее число людей так и не оценило. Опять Microsoft пришлось в более поздних версиях Microsoft Office предупреждать пользователей и по умолчанию отключать исполнение подозрительных макросов.

Особую заботу у специалистов по безопасности вызывают беспроводные технологии. Тоже наглядный пример, как на обратной стороне красивой рекламной картинки (благостного вида менеджер перемещается свободно по офису с ноутбуком и чашкой кофе) – конкретные инструкции по взлому Wi-Fi сетей. Появился даже новый вид спорта – вардрайвинг (англ. wardriving), смысл которого – в поиске и взломе уязвимых точек доступа беспроводных сетей Wi-Fi хакерами (как правило на автомобилях – отсюда и название), оснащенными переносным компьютером с Wi-Fi-адаптером.

Поскольку трафик, передаваемый по радиоканалу, в принципе, не защищен от прослушивания и изменения, в технологии Wi-Fi изначально был встроен механизм шифрования канала. Первым протоколом стал WEP (1999 год), который использовал 40-битные ключи и довольно распространенный алгоритм RC4. Уже тогда перебор всех ключей (их около 500 млрд) не представлял проблем для обычного персонального компьютера.

Производители оборудования перешли на 104-битные ключи, полный перебор стал исключен, и тогда за дело взялись криптоаналитики, которые обнаружили уязвимость в самом алгоритме RC4. Результат – возможность взлома за часы и даже минуты. В 2003 году альянс Wi-Fi принял новый протокол – WPA (затем в 2004 году – WPA2), а прежний WEP признал непригодным с точки зрения безопасности. Но, как показывает опыт, от врожденной уязвимости избавиться очень трудно, требуется или замена/обновление программно-аппаратных средств или ручные операции со стороны пользователей, к которым те совершенно не склонны. На волне интереса к Wi-Fi было закуплено много оборудования, которое работает только с WEP, и просто так выбрасывать его мало кому хочется, так же как и вчитываться в содержимое сайтов производителей, предлагающих инструкции по повышению безопасности.

Довольно интересны в этом плане результаты вардрайвинга, который провела «Информзащита» в Москве в 2005 году: только 5% использовали более защищенный протокол WPA, 12% всех точек доступа использовали настройки «по умолчанию» (весьма небезопасные). То есть, производители от потребителей добились того, чего хотели, – цепочки «купи, включи и ни о чем не думай».

К слову, нет гарантии, что и WPA небезгрешен. Например, в ноябре прошлого года был представлен способ, как за 15 минут найти ключ для чтения и даже навязывания данных, передаваемых от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. В принципе, современный WPA2 считается пока неуязвимым, но надолго ли?

Конечно, не стоит драматизировать принципиальную противоречивость удобства и безопасности. Перечень рассмотренных примеров не претендует на полноту, да и в каждой из перечисленных уязвимостей гораздо больше нюансов, чем это можно изложить в статье. Цель этой статьи – лишь показать, что источником проблем безопасности становятся избыточные удобства, которые зачастую даже и не востребуются людьми.

Возвращаясь к некомпьютерным областям, где на первое место ставится безопасность, а не удобство (автомобильная, авиационная, пожарная безопасность), глядя на бесконечные новости об инцидентах компьютерной безопасности, возникает здравая мысль, а почему бы эту гегелевскую философию по-маркситски не поставить «с головы на ноги».

**Литература**

1. Мельников, В. Защита информации в компьютерных системах. – М. : Финансы и статистика, 1997.

2. Мельников, Д.А. Информационные процессы в компьютерных сетях. – М. : Кудиц – Образ, 1999.

3. Щербо, В.К. Стандарты вычислительных сетей. – М. : Кудиц. – Образ, 2000.

4. Спесивцев, А.В. Защита информации в ПЭВМ. – М. : Мир, 1991.