

# Клавиатура с усилителем пароля

Простое устройство, решающее проблемы простых паролей.



**К**акие пароли зачастую мы видим в таких ответственных местах, как сетевое оборудование, базы данных, серверы или у пользователей на машинах, почтовых ящиках, форумах? «111», «000» и подобные.

Повозмущавшись таким безобразием, давайте задумаемся и посмотрим на наши отделы и фирмы, где мы работаем, что мы видим? Пароли, записанные на чем попало и чем угодно. Разноцветные стикеры на мониторах с именами домашних животных, «мам», «пап», интернациональный «qwerty» и т. п. Критикуем провайдеру, а сами «по понедельникам» ходим и сдираем эти стикеры, делаем выговоры пользователям, сообщаем о положении дел начальству, которое кивает головой, но в то же время просит поставить на корпоративную почту пароль попроще.

## Проблемы насущные

Простые пароли стали предметом шуток и баек, которые, правда, вызывают кривую усмешку у системных администраторов — смеемся сами над собой. Винить пользователей в том, что раз в месяц они не могут запомнить 3-4 пароля, состоящие из невнятных символов? Можно придумывать ухищрения, можно придумать алгоритм, упростить задачу, но все равно проблема останется. В России еще только набирает обороты «социальный хакинг», когда в call-центр компании звонит злоумышленник, представляясь сотрудником службы поддержки, просит сообщить конфиденциальную информацию, и уставший человек «на автомате» сообщает ему эту информацию. Сколько электронных писем с поддельным адресом отправителя приходят с просьбами сообщить закрытую информацию? В Европе эти проблемы в полном разгаре, только от банковских карт украдено множество паролей. И это уже в порядке вещей. Кевин Митник пишет книги об успешном «со-

циальном хакинге», злоумышленники уже не развлекаются на просторах сети, они просто воруют деньги.

Как хотелось бы найти одно простое решение, которое смогло бы облегчить жизнь нам, системным администраторам, а пользователям позволяло не забивать голову лишней информацией, и при всем этом повысить безопасность наших предприятий и офисов.

Что можно придумать для усиления паролей? Первое, что может прийти в голову, это решение с идентификацией отпечатков пальцев, простое и дешевое, правда с массой недостатков. Один из самых значимых, в российских условиях минус, заключается в том, что при резком перепаде температур (на улице -10, в кабинете +20) отпечаток деформируется, и пользователь долго не сможет получить доступ к необходимой информации. Смарт-карты? USB-брелки? Это хорошие технологии, но все они зависят от операционных систем и оборудования, плюс эти системы слишком сложны и специфичны. Все-таки, есть ли простое, прозрачное решение для усиления всех паролей?!

## Простое решение

Выход всегда есть. На российском рынке появилась не совсем обычная клавиатура, решающая проблемы простых паролей. Что собой представляет это устройство? Клавиатура выглядит так же, как и все, работа на ней ничем не отличается от других таких же устройств, но когда необходимо аутентифицировать себя и ввести пароль на каком-то ресурсе или устройстве... Смело набрав пароль «12345», можно быть уверенным, что он абсолютно «неподбираем», его бесполезно «подсматривать», так же как и передавать по телефону, даже стикер на мониторе не выдаст конфиденциальную информацию вошедшему в офис злоумышленнику. Как же это возможно?!

Все просто, перед вводом пароля достаточно нажать специальную кнопку на клавиатуре, и она переводится в режим усиления пароля, в котором при нажатии любой одной клавиши компьютеру передается запрограммированная последовательность символов, как будто вы нажали не одну, а последовательно несколько клавиш. Например, если ввести пароль «12345», то в компьютер будет передано что-то вида «uH9%0!jiSLo\*3ejK(d83». Даже сам пользователь может не знать свой настоящий пароль. После ввода пароля клавиатура также нажатием специальной кнопки выводится из режима усиления пароля. Но откуда берется подобная последовательность символов и каково их количество? Данный параметр заранее программируется специалистом, длина последовательности на каждую клавишу составляет от 2 до 10 символов и включает в себя последовательность букв обоих регистров, цифр и специальных символов, сгенерированных случайным образом. Все просто, прозрачно для пользователя, при этом на предприятии или в офисе безопасность повышается в разы. Не нужно ломать голову над паролем, даже любимый qwerty окажется неприступной стеной из 30-40 символов для злоумышленника. Не говоря уже о множестве плюсов данного решения: можно забыть о раскладках клавиатуры (пароля из цифр и специальных символов будет достаточно), устройство не зависит от ОС и драйверов. Где же достать подобную клавиатуру? На сайте производителя [www.antihacking.ru](http://www.antihacking.ru) можно найти полную справочную информацию о ней. Особенно приятно, что это устройство изобретено, запатентовано в России и защищается российским законодательством об интеллектуальной собственности. ●

Иван Максимов.  
На правах рекламы