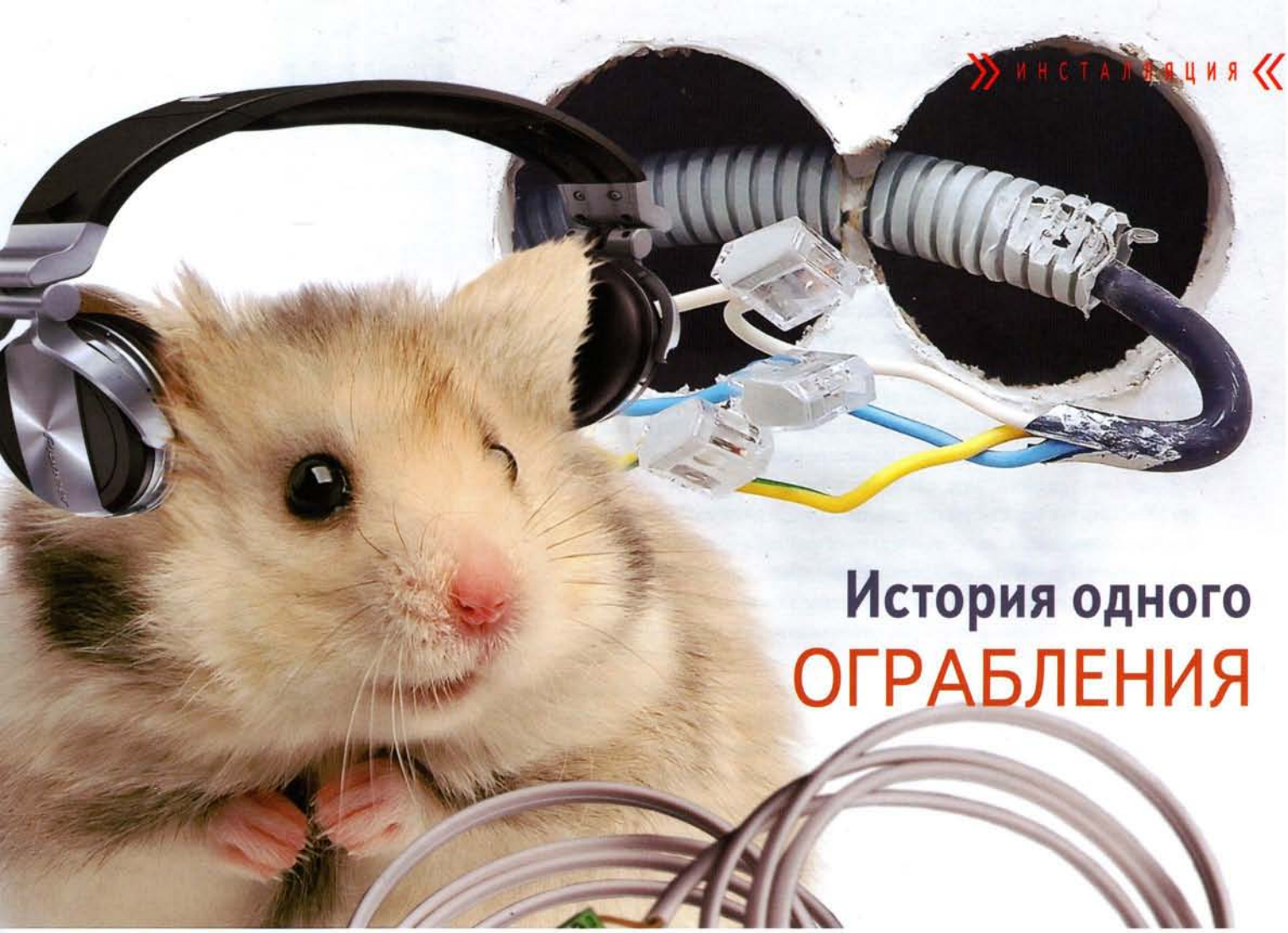


История одного ОГРАБЛЕНИЯ

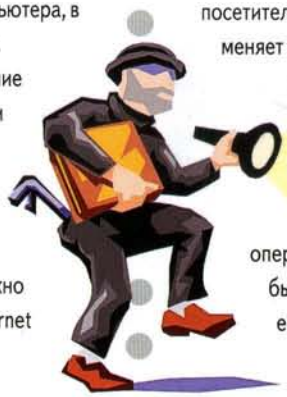
Алексей ОМЕЛЬЯНЧУК,
эксперт

Жила была компания, не большая, но и не маленькая, и был у нее дом, и был в том доме склад с товарами. И, конечно, в доме том была весьма продуманная и вполне современная система охранно-пожарной сигнализации и даже контроля доступа. И был человек, эту систему обслуживавший.

И вот обиделся этот человек на компанию, решил, что зарплата маловата, и уволился. И, видать, нехорошо они расставались, обида осталась. Начальник компании, конечно, тут же нанял другого администратора систем и велел ему пароль доступа сменить. И тот сменил. Но был он человек новый, не очень опытный, сменил только основной пароль, с помощью которого со своего компьютера, в сеть компании подключенного, всей системой управлял.

А того, прежнего, уволенного человека нашли нехорошие люди и соблазнили большими посулам – дескать, помоги нам и с обидчиками своими посчитаешься. И согласился он (знания у него были, а вот стыда и совести, видать, не хватало).

А система была установлена хоть и современная, с немалой историей и с большими возможностями. Ее можно было программировать не только с компьютера, в Ethernet подключенного, но и просто с пульта, включенного в линию RS485, по всему зданию проложенную. И пароль там нужен совсем другой, не как в компьютере – длинный и сложный, а всего 4 циферки.



И вот пришел этот нехороший прежний человек вроде как по делу в старую свою компанию, незаметно подключился к линии RS485 где-то возле туалета (он же сам ее прокладывал, хорошо знал, где она проходит) и запрограммировал систему, чтобы она впустила злодеев в самый-самый главный склад, пока никто не видит. И пустила система злодеев, и вынесли они товару разного в количествах немереных.

Мораль сей истории многогранна. Кадровик и психолог, наверное, сделают свои выводы, я же могу дать рекомендации технарям по системам охраны и тем, кто их контролирует.

Во-первых, следует помнить, что в любую систему есть множество «черных входов» помимо главного административного интерфейса.

Например, широко известна такая дыра в безопасности: многие системы контроля доступа используют стандартные базы данных. У этих баз данных есть собственный пароль администратора (исключительно для администрирования самой базы данных), зная который обычно можно как минимум прочитать всю базу данных, а иногда и нетрудно догадаться, как подправить данные, например, чтобы ваша карточка посетителя открыла сейф с деньгами. Как правило, этот пароль вообще никто не меняет и он остается «по умолчанию» стандартным для данной СУБД. Причем для этого обычно не нужен физический доступ к компьютеру с базой данных.

Конечно, пароли базы данных можно поменять и запретить доступ к ней с других компьютеров кроме компьютера оператора бюро пропусков, но это же надо не забыть сделать.

Если в системе есть компьютер, у него есть пароль (или много паролей) к операционной системе. Внешне это может быть незаметно, компьютер может быть настроен на автоматический запуск с минимальными правами, но у него есть пароль администратора компьютера (или локальной сети). На первый

взгляд это не имеет отношения собственно к системе охраны, но, имея такой доступ, легко поставить широко доступные программы перехвата клавиатурного ввода и копирования экрана. Да, обычно просто достаточно поставить галочку «разрешить удаленный доступ», и общеизвестными средствами самой операционной системы злоумышленник перехватит управление уже после того, как вы ввели суперсекретный пароль к суперсекретной программе управления охранной сигнализацией. Да, этот пароль также должен быть сменен при увольнении администратора системы. А лучше бы и проконтролировать запрет доступа ко всем компьютерам системы по сети. На практике компьютеры охранного назначения стараются вообще физически отключить от общей сети. Но к этой специальной «охранной» компьютерной сети все рано останется доступ, например, с компьютера, установленного в дальнем КПП, перед которым скучает одинокий вахтер. Обратите внимание: специализированное программное обеспечение систем охраны обычно само не вносит никаких изменений в общесистемные настройки – уж очень разными они могут быть в разных случаях. Смена паролей операционной системы и настройка фаерволлов – отдельная забота администратора системы.

Но пароли операционной системы – далеко не все. Например, пароли, устанавливаемые Windows, обрабатывает только сама Windows. Достаточно загрузить компьютер с флэшки с Linux, и вы администратор на вашем Windows-компьютере. Поэтому разумным решением является физическое ограничение доступа ко всем компьютерам системы безопасности, или (для параноиков) применение средств шифрования жесткого диска.

И возвращаясь к низкоуровневым интерфейсам. Уже упомянутая возможность подключиться не только через Ethernet, но и с пульта (эмулятора пульта) через RS485 или другой интерфейс существует во многих системах. И пароль там, как правило, не тот, который используется для обычной работы с компьютера. И если такая возможность вообще не использовалась после монтажа оборудования, то пароль с пульта с большой вероятностью остался тем, который «по умолчанию» установлен на заводе и известен любому, знакомому с аппаратурой.

Еще во многих системах есть, например, возможность завести «мастер-карту», которая позволяет регистрировать новые карты в системе. Если система большая и стоит компьютер в бюро пропусков, такие средства не нужны. Но они могут быть предусмотрены для простых вариантов комплектации системы, а в большой системе эти средства – дыра в безопасности. Конечно, эту дыру можно закрыть, отключить, запретить, если, конечно, об этом кто-то вспомнит.

В заключение рекомендации для начальника службы безопасности. Не обязательно лично разбираться в аппаратуре. Пусть администратор системы заранее составит список всех способов, с помощью которых можно что-то изменить в системе, и укажет все пароли, которые при этом могут потребоваться. Этот список можно проверить у стороннего специалиста, проконсультироваться с производителями аппаратуры. Понятно, что все пароли должны храниться в сейфе начальника СБ на случай, если администратор, не дай бог, попадет под трамвай. Желательно проанализировать этот список на предмет, «какой способ доступа можно совсем заблокировать» (но хотя бы один резервный вариант стоит оставить на случай, если, например, неожиданно отказал основной компьютер). Все эти пароли по списку должны быть сразу изменены при увольнении предыдущего администратора (для того и полный список, чтобы не забыть поменять все).