



Найдена уязвимость в безопасности некоторых SIM-карт, дающая возможность установить сторонний контроль над мобильным телефоном, сообщает издание The New York Times.

Основатель Security Research Labs Карстен Нол (Karsten Nohl) заявил, что технология шифрования, которая применяется в некоторых SIM-картах, имеет серьезную уязвимость. "Дыра" в безопасности позволяет злоумышленникам получить 56-значный цифровой ключ доступа к чипу устройства, зная который, можно заразить мобильный телефон вирусом, послав его в простом текстовом сообщении.

В качестве эксперимента Карстен Нол таким способом получил управление мобильным телефоном "жертвы" и смог совершать от ее имени покупки посредством платежных систем. Вся операция заняла у "взломщика" не более двух минут, при этом использовался обычный персональный компьютер.

Прослушивать разговоры, читать переписку, скопировать всю информацию с SIM-карты, полностью украсть "цифровую личность" владельца телефона — все это можно сделать, имея в своем распоряжении упомянутый цифровой ключ. По оценке эксперта, подобного рода атакам рискуют подвергнуться порядка 750 миллионов устройств по всему миру.

Карстен Нол не сообщил, SIM-карты каких операторов наиболее уязвимы для взлома. По его словам, данная информация не будет озвучена и на конференции Black Hat, посвященной вопросам безопасности, которая пройдет в августе. Сравнительный анализ защиты различных SIM-карт можно ожидать в декабре 2013 года, в рамках хакерской конференции Chaos Communication Congress в Гамбурге.

[РИА "Новости"](#)