АНАЛИЗ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Лисица Е.В., 5 курс,
Урбанович П.П.,д.т.н, профессор,
УО «Белорусский государственный технологический университет»

При проектировании современных криптографических систем применяют подход, основанный на *принципе Керкхоффса* (Kerckhoffs). Согласно этому принципу алгоритм криптографического преобразования является открытым и известным любому противнику, а секретность шифра обеспечивается секретностью ключа шифрования.

На этом принципе основан протокол Кинцеля-Кантера. Потенциальному противнику (intruder), известно строение TPM-машины (tree parity machine) и алгоритм, применяемый отправителем и получателем для обмена информацией, а также значения вектора входных и выходных значений на каждом шаге. При этом стойкость алгоритма на основе нейросетевых технологий заключается в невозможности атакующей стороны влиять на процесс обновления весов отправителя и получателя. Из исследований В. Кинцеля и И. Кантера следует, что при простой атаке количество персептронов в TPM-машине, равное 2, является оптимальным для отправителя и получателя, так как они успевают синхронизироваться за время на порядок быстрее атакующей стороны.

Однако А. Митягиным и А. Климовым были предложены три способа взлома нейросетевого протокола обмена ключом: с помощью *генетической атаки* (genetic attack), *геометрической атаки* (geometric attack) и *мажоритарной атаки* (majority attack). На основе анализа эффективности этих методов были сделаны выводы о безопасности нейронного протокола обмена ключом.

Поскольку для шифровальных систем на основе нейросетевых технологий параметром, обеспечивающим безопасность передачи информации, является синаптическая глубина L нейронных сетей, то увеличение ее значения является необходимым условием для снижения вероятности успешной атаки. Так для геометрической и мажоритарной атак увеличение значения синаптической глубины является достаточным для предотвращения атаки.

Рассматриваемые методы можно улучшить, если добавить в них *генетический алгоритм*, который выбирает оптимальные нейронные сети. Так как криптосистема основана на биологическом понятии нейронных сетей, А. Климов и А. Митягин применили биологически мотивированную атаку, основанную на генетических алгоритмах. В данной атаке они моделировали большую совокупность нейронных сетей с той же самой структурой, как у отправителя и получателя. Сети, значения выходов которых равны значению выхода сети отправителя, остаются и размножаются, в то время как неудачные сети удаляются.

Для рекомендованного В. Кинцелем и И. Кантером выбора параметров (количество персептронов $K = 3$, количество входов $N = 101$, $L = 3$), А. Климов и А. Митягин пробовали атаку с $M = 2500$ сетей, и больше чем в 50% их тестов, по крайней мере, одна из сетей атакующей стороны синхронизировалась с отправителем раньше, чем отправитель и получатель. Из результатов их исследований также следует, что генетическая атака особенно эффективна для вариантов, при которых используются небольшие значения K.

Таким образом, при генетической атаке использование нейросетевого протокола обмена ключом является небезопасным.