***Ж. Сайлаукызы, магистр техники и технологии,***

***М.М.Коккоз к.т.н., доцент***

***(КарГТУ, Казахстан г.Караганда)***

**ВЗЛОМ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ С ПОМОЩЬЮ КРИПТОАНАЛИЗА**

Стойкость любой криптосистемы зависит от вида совершенной на нее атаки, т.е. к одному виду атак она может быть устойчива, а к другим нет. Другими словами, «криптосистема X» может считаться стойкой к атаке Y, но не стойкой по отношению к атаке Z. Существует множество активных атак, которые можно разделить на три основных вида:

* атака на основе подобранного открытого текста;
* атака на основе подобранного зашифрованного текста;
* атака на основе адаптивно подобранного зашифрованного текста.

Атака на основе подобранного открытого текста (*chosen-plaintext attack - CPA*). Злоумышленник выбирает исходное сообщение и отправляет его на шифрование для того чтобы получить зашифрованный текст. Задачей злоумышленника является – взломать криптосистему, используя перехваченные пары открытого и зашифрованного текстов.[1]

Атака на основе подобранного зашифрованного текста (*chosen-ciphertext attack - CCA*). Злоумышленник выбирает зашифрованные сообщения и отправляет его расшифровывать для того чтобы получить исходные сообщение. Целью злоумышленника является взломать криптосистему, используя перехваченные пары открытого и зашифрованного текстов. Злоумышленник достигает успеха при условии, что он смог вычислить ключ и, не используя постороннюю помощь, может получать секретную информацию из зашифрованного текста.

Атака на основе адаптивно подобранного зашифрованного текста (*adaptive* *ciphertext attack – CCA2*). Это одна из разновидностей атак ССА, где услуги по расшифровке применимы для всех зашифрованных текстов, кроме заданного.

Такие атаки можно проходить по следующим сценариям.

В атаке, которая основывается на подборе открытого текста, злоумышленник обладает блоком шифрования.

В атаке, которая основывается на подборе зашифрованного текста, злоумышленник владеет ограниченным доступом к блоку расшифровки, т.к. доступ к блоку закрывается, после нескольких попыток, и тогда расшифровку необходимого текста злоумышленник должен выполнить самостоятельно.

В атаке, которая основывается на адаптивно подобранном зашифрованном тексте, злоумышленник обладает блоком расшифровка столько, сколько ему необходимо, но, как и в предыдущей атаке, расшифровку требуемого текста необходимо выполнять самостоятельно.

Все вышеописанные атаки базируются на том, что злоумышленник не знает криптографический ключ.

Такие атаки как СРА и ССА изначально были предназначены для криптоанализа симметричных криптосистем. Такой криптоанализ предназначен для взлома криптосистем используя пары, состоящие из открытых и зашифрованных сообщений, которые получают в ходе атаки [2]. Позже они было адаптированы под асимметричные криптосистемы.

Услуги по шифрованию в асимметричных криптосистемах доступны любому желающему, так как при наличии открытого ключа можно получить тотальный контроль над алгоритмом шифрования. Другими словами, криптосистему с открытым ключом можно взломать, используя атаку которая основывается на подборе открытого текста. Таким образом, атаку на криптосистему с открытым ключом без использования блока расшифровки, можно назвать атакой СРА.

Атака ССА очень сильно ограничивает возможности злоумышленника. В приложении пользователь, может подвергнуться атаке (т.е. пользователь, к которому обратились расшифровать сообщение), даже не знает об этом. Отсюда следует, что пользователь не знает, когда необходимо прекратить расшифровку. Обычно, предполагается, что пользователь наивен и не подозревает о существовании злоумышленника, а это приводит к тому, что услуги по расшифровке сообщений доступны постоянно. С другой стороны, криптосистема с открытым ключом должна быть устойчива к атакам СРА, т.к. злоумышленник может сам зашифровать подобранные открытые сообщения. Из этого следует, что логичнее уделять больше внимания атакам, которые основаны на ССА.

**Библиографический список**

1. Смарт Н. «Криптография»: Пер. с англ. – М.:Техносфера, 2005. – 528 с.
2. D.R.Stinson. Cryptography: Theory and Practice. CRC Press, Inc., 1995
3. Смарт Н. «Криптография»: Пер. с англ. – М.:Техносфера, 2005. – 528 с.