Алиев Александр Тофикович
Государственное образовательное учреждение высшего профессионального образования «Донской государственный технический университет».
E-mail: A.T.Aliev@mail.ru.
344000, г. Ростов-на-Дону, пл. Гагарина, 1.
Тел.: +79094205581.

Aliev Alexander Tofikovich
State educational institution of higher education “Don State Technical University”.
E-mail: A.T.Aliev@mail.ru.
1, Gagarin Square, Rostov-on-Don, 344000, Russia.
Phone: +79094205581.

УДК 004.056.55

А.Ф. Чипига

ОБОСНОВАНИЕ ВОЗМОЖНОСТИ СОХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ В СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧА ШИФРОВАНИЯ

Показана возможность сохранения конфиденциальности данных при компрометации ключа шифрования за счет использования энергетической и структурной скрытности сигналов на физическом уровне эталонной модели взаимосвязи открытых систем.

Информационная безопасность систем связи; энергетическая скрытность; структурная скрытность; информационная скрытность.

A.F. Chipiga

THE SUBSTANTIATION OF A POSSIBILITY TO MAINTAIN CONFIDENTIALITY IN SYMMETRIC CRYPTOSYSTEMS IN CASE OF A COMPROMISE OF AN ENCRYPTION KEY

The possibility of maintaining confidentiality in symmetric cryptosystems in case of a compromise of an encryption key using energetic and structural signal hiding on physical layer of OSI reference model was shown.

Information security of communications; energetic signal hiding; structural signal hiding; informational hiding.

Введение. Постановка задачи. Рост объемов конфиденциальной информации, передаваемой по незащищенным каналам связи, привел к широкому применению криптографических методов защиты. При этом предполагается, что криптография должна обеспечить такую защиту конфиденциальной информации, что даже в случае ее перехвата противником и обработки любыми способами с использованием современных и перспективных средств вычислительной техники она не должна быть дешифрована в течение нескольких десятилетий. Криптографическая стойкость системы шифрования должна определяться исключительно криптографической стойкостью ключа.

Проводимые мероприятия по противодействию угрозам безопасности информации приводят к значительному снижению возможности неправомерного овладения охраняемыми сведениями. Однако статистика говорит о том, что до

82% угроз совершается собственными сотрудниками фирмы при их прямом или опосредованном участии [1]. Здесь же констатируется тот факт, что несанкционированный доступ к охраняемым сведениям путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок составляет 24 %. Следовательно, можно предположить, что одной из форм незаконного получения конфиденциальных данных является получение противником информации о содержании криптографического ключа. При этом перед владельцами грифованных данных возникает проблема: как сохранить заданный уровень конфиденциальности при передаче данных по незащищенным каналам связи при условии, что противнику известен ключ дешифрования? Важность проблемы обуславливается еще и тем, что прослушивание канала связи является непременным условием для проведения большинства атак [2].

Решение задачи. В [3] введено понятие информационной безопасности системы связи, причем под охраняемыми сведениями системы связи понимается информация о структуре, управлении, процессах, секретная информация, циркулирующая в технических средствах передачи информации, которые через демаскирующие признаки функционирования системы связи, параметры техники и объектов связи подлежат защите от технических средств разведки противника. Количественной оценкой защищенности охраняемых сведений системы связи является вероятность сохранения конфиденциальности охраняемых сведений, включающая учет уровня разведывательной защищенности систем связи от технических средств разведки и уровня скрытности управления связью.

Поэтому конфиденциальность передачи сообщений по системе связи может быть достигнута путем обеспечения [3]:

1) энергетической скрытности сигналов-переносчиков информации;
2) структурной скрытности этих сигналов;
3) информационной скрытности самого сообщения.

Энергетическая скрытность характеризует способность противостоять мерам, направленным на обнаружение сигнала разведывательным приемным устройствам, а структурная скрытность – степень затруднения определения структуры обнаруженного сигнала. Информационная скрытность определяется стойкостью криптографического ключа.

Пусть $К$ – событие, заключающееся в сохранении конфиденциальности передачи сообщений по системе связи, $ЭС$ – событие, заключающееся в обеспечении энергетической скрытности сигналов-передатчиков, $СС$ – событие, заключающееся в обеспечении структурной скрытности сигналов, $ИС$ – событие, заключающееся в обеспечении информационной скрытности сообщения.

В этом случае количественная оценка сохранения конфиденциальности передачи сообщений по системе связи будет носить вероятностный характер и может быть задана функцией

$$P(K) = f\{P(ЭС), P(СС), P(ИС)\},$$
$$0 \le P(K) \le 1, 0 \le P(ЭС) \le 1, 0 \le P(СС) \le 1, 0 \le P(ИС) \le 1. \quad (1)$$

где $P(K)$ – вероятность сохранения конфиденциальности передаваемых сведений; $P(ЭС)$ – вероятность обеспечения энергетической скрытности сигналов;

$P(CC)$ – вероятность обеспечения структурной скрытности; $P(ИС)$ – вероятность обеспечения информационной скрытности.

Следовательно, криптографические преобразования обеспечивают высокий уровень значения $P(ИС)$, но не только ими определяется высокий уровень показателя $P(K)$. Поэтому решение проблемы обеспечения заданного уровня конфиденциальности данных, циркулирующих в сети связи при компрометации ключа дешифрования, будет находиться в плоскости обеспечения высокой энергетической и структурной скрытности передаваемых сигналов.

События $ЭС, CC, ИС$ являются совместными, так как появление каждого из них не зависит от того, появилось ли другое событие, или нет. Считаем, что

$$K = ЭС + CC + ИС, \tag{2}$$

тогда

$$\begin{aligned} P(K) = {} & P(ЭС) + P(CC) + P(ИС) - P(ЭС) \cdot P(CC) - \\ & - P(ЭС) \cdot P(ИС) - P(CC) \cdot P(ИС) + P(ЭС) \cdot P(CC) \cdot P(ИС) \end{aligned} \tag{3}$$

при определенных условиях, таких, чтобы $P(K) \neq 0$. Найдем эти условия и определим окончательное значение $P(K)$.

В выражении (3) возможно, что любая его составляющая будет равна 0, т.е. $P(ЭС) = 0 \vee P(CC) = 0 \vee P(ИС) = 0$. Поэтому необходимо исключить вероятность того, что $P(K) = 0$. Учитывая то, что перестановки из элементов $P(ЭС), P(CC)$ и $P(ИС)$ в произведении дают одно и то же значение, получим матрицу A возможных произведений, множителями которой являются элементы строк:

$$A = \begin{pmatrix} 0 & 0 & P(ЭС) \\ 0 & 0 & P(CC) \\ 0 & 0 & P(ИС) \\ 0 & P(ЭС) & P(CC) \\ 0 & P(ЭС) & P(ИС) \\ 0 & P(CC) & P(ИС) \\ P(ЭС) & P(CC) & P(ИС) \end{pmatrix}. \tag{4}$$

Используя выражение (4), произведения элементов строк могут быть представлены следующим образом:

$$P_i(K) = \prod_{j=1}^{3} a_{ij}, \tag{5}$$

где i – номер строки, $i = \overline{1,7}$, j – номер столбца, $j = \overline{1,3}$, a_{ij} – элемент матрицы A. Тогда $P(K)$ примет вид:

$$P(K)=\begin{cases} P(ЭС), & \text{если } P(СС)=0,\ P(ИС)=0. \\ P(СС), & \text{если } P(ЭС)=0,\ P(ИС)=0. \\ P(ИС), & \text{если } P(ЭС)=0,\ P(СС)=0. \\ P(ЭС)+P(СС)-P(ЭС)\cdot P(СС), & \text{если } P(ИС)=0. \\ P(ЭС)+P(ИС)-P(ЭС)\cdot P(ИС), & \text{если } P(СС)=0. \\ P(СС)+P(ИС)-P(СС)\cdot P(ИС), & \text{если } P(ЭС)=0. \\ P(ЭС)+P(СС)+P(ИС)-P(ЭС)\cdot P(СС)- & \text{если } P(ЭС)\neq 0, \\ -P(ЭС)\cdot P(ИС)-P(СС)\cdot P(ИС)+ & P(СС)\neq 0, \\ +P(ЭС)\cdot P(СС)\cdot P(ИС), & P(ИС)\neq 0. \end{cases}$$

Выводы. Анализ последнего выражения позволяет сделать вывод, что только в случае не обеспечения всех трех составляющих конфиденциальности передачи сообщений по линии связи $\left(P(ЭС)=0, P(СС)=0, P(ИС)=0\right)$ конфиденциальность передачи сообщений по системе связи может быть не обеспечена. Если учесть, что информационная скрытность обеспечивается применением криптографических методов защиты информации, то даже в случае компрометации ключа заданный уровень конфиденциальности может быть обеспечен путем достижения заданного уровня энергетической и структурной скрытности сигналов на физическом уровне эталонной модели взаимосвязи открытых систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ярочкин В.И.* Информационная безопасность: Учебник для студентов вузов. В.И. Ярочкин. – М.: Академический проспект: Фонд «Мир», 2003. – 640 с.
2. Обеспечение информационной безопасности в экономической и телекоммуникационной сферах. Коллективная монография. / Под ред. Е.Н. Сухарева. Кн. 2. – М.: Радиотехника, 2003. – 216 с.
3. Общесистемные вопросы защиты информации. Коллективная монография / Под ред. Е.Н. Сухарева. Кн. 1. – М.: Радиотехника, 2003. – 296 с.

Чипига Александр Федорович
Северо-Кавказский государственный технический университет.
E-mail: zik@ncstu.ru.
355003, г. Ставрополь, ул. Морозова, 105, кв. 15.
Тел.: 89624441070.

Chipiga Alexander Fedorovich
North Caucasus State Technical University.
E-mail: zik@ncstu.ru.
App. 15, 105, Morozova street, Stavropol, 355003, Russia.
Phone: +79624441070.