2.2. Понятие стойкости шифра

В далекие времена надежность сохранения информации в тайне определялась секретностью самого метода преобразования. Однако секретность алгоритма принципиально не может обеспечить его *безусловную стойкость***,** т. е. невозможность чтения криптограммы противником, обладающим бесконечными вычислительными ресурсами. Поскольку секретные алгоритмы не доступны для проведения широкомасштабных криптоаналитических исследований, то по сравнению с открытыми алгоритмами имеется значительно более высокая вероятность того, что впоследствии будут найдены уязвимые места и эффективные способы их взлома. В связи с этими обстоятельствами в настоящее время наиболее широко используются открытые алгоритмы, прошедшие длительное тестирование и обсуждение в открытой криптографической литературе.

Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации сравнительно малого размера, называемой *секретным ключом***.** Ключ используется для управления процессом криптографического преобразования (шифрования) и является легко сменяемым элементом криптосистемы. Ключ может быть заменен пользователями в произвольный момент времени, тогда как сам алгоритм шифровании является долгосрочным элементом криптосистемы и связан с длительным этапом разработки и тестирования.

Голландский криптограф Керкхофф (1835—1903) впервые сформулировал правило стойкости шифра**,** в соответствии с которым:

- весь механизм преобразований считается известным злоумышленнику;
- надежность алгоритма должна определяться только неизвестным значением секретного ключа.

Второе требование означает, что оппонент не сможет разработать методы, позволяющие снять защиту или определить истинный ключ, за время существенно меньшее, чем время *полного (тотального) перебора* всего множества возможных секретных ключей. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации. Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Безопасность, обеспечиваемая традиционной криптографией, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические

закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Принято различать криптоалгоритмы по степени доказуемости их безопасности. Существуют *безусловно стойкие, доказуемо стойкие* и *предположительно стойкие криптоалгоритмы*. Безопасность *безусловно стойких криптоалгоритмов* основана на доказанных теоремах о невозможности раскрытия ключа. Строго говоря, безусловно стойкими называются шифры (по Шеннону – совершенно секретными), для которых криптоаналитик не может улучшить оценку исходного сообщения *M* на основе знания криптограммы C по сравнению с оценкой при неизвестной криптограмме. При этом предполагается, что криптоаналитик обладает бесконечными вычислительными ресурсами. Примером безусловно стойкого криптоалгоритма является система с разовым использованием ключей (шифр Вернама) или система квантовой криптографии, основанная на квантовомеханическом принципе неопределенности.

Криптосистемы второго типа характеризуются тем, что по мере того, как объем доступной криптоаналитику криптограммы возрастает при определенном значении $n=n_0$, существует единственное решение криптоаналитической задачи. Минимальный объем криптограммы, для которого имеется единственное решение, называется *расстоянием единственности*. В случае ленты однократного использования $n_0 \to \infty$. При конечной длине секретного ключа значение n_0 конечно. Заранее известно, что по криптограмме, имеющей размер больше расстояния единственности можно найти единственное решение криптоаналитической задачи. Однако для криптоаналитика, обладающего ограниченными вычислительными ресурсами, вероятность найти это решение за время, в течение которого информация представляет ценность, чрезвычайно мала (10^{-30} и менее). Стойкость *доказуемо стойких криптоалгоритмов* определяется сложностью решения хорошо известной математической задачи, которую пытались решить многие математики и которая является общепризнанно сложной. Примером могут служить системы Диффи-Хеллмана или Ривеста-Шамира-Адельмана, основанные на сложностях соответственно дискретного логарифмирования и разложения целого числа на множители.

Предположительно стойкие криптоалгоритмы основаны на сложности решения частной математической задачи, которая не сводится к хорошо известным задачам и которую пытались решить один или несколько человек. Задачи такого типа называются трудными или вычислительно сложными, а об их решении говорится, что оно является вычислительно нереализуемым (или вычислительно неосуществимым). Примерами могут криптоалгоритмы *ГОСТ 28147-89, DES, FEAL.*

Клод Шеннон ввел понятия диффузии и конфузии для описания стойкости алгоритма шифрования.

Диффузия – это рассеяние статистических особенностей и закономерностей незашифрованного текста в широком диапазоне статистических особенностей и закономерностей зашифрованного текста. *Конфузия* – это уничтожение статистической взаимосвязи между зашифрованным текстом и ключом.