УДК 681.322.067

НЕКОТОРЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ В ПУБЛИЧНЫХ ОРГАНИЗАЦИЯХ И УЧРЕЖДЕНИЯХ

Вацьковски Казимеж Станиславович,
д.е.н., проф., зав. кафедрой информатических систем Варшавского технологического университета «Варшавская политехника», Польша,
Гордиенко Лариса Юрьевна,
к.э.н., доцент, доцент кафедры государственного управления, публичного администрирования и региональной экономики ХНЭУ им. С. Кузнеца

На современном этапе развития общества, характеризующегося трансформацией социально-экономических и политических систем, усложняются и ускоряются глобализационные процессы и вызовы национальным системам и отдельным ее составляющим (предприятиям, учреждениям и т.п. организационным формам).

В современном мире при управлении социально-экономическими и политическими системами и их составляющими наблюдается процесс усиления конкурентной борьбы между странами на всех уровнях, как общенациональном, отраслевом, так и организационном, что вызывает необходимость защиты информации.

Потребность у людей скрывать и маскировать то, что они писали, появилась вскоре после овладения искусством письма. На ранних этапах развития письменности были предприняты попытки замаскировать само существование сообщения, а не его содержание. Со временем появились первые простые заменительные шифры, суть которых состояла в обмене одной буквы

на другую, способом, известным только инсайдерам. Когда возникли первые государственные организмы, все более важную информацию приходилось отправлять в письменном виде на большие расстояния, что привело к использованию все более сильных и более сложных шифров. В настоящее время алгоритмы шифрования от передовых механических систем Второй мировой войны (например, машина шифрования Лоренца, Энигма) были перенесены на компьютеры или технически имплементированы в специализированных электронных устройствах.

В процессе эволюции практической деятельности в сфере информационной безопасности возникла необходимость в теоретических исследованиях, что привело к появлению такой теоретической области знаний как криптография, которая, в свою очередь, является частью криптологии, области знаний о передаче информации способом, защищенным от несанкционированного доступа.

Голландский языковед и криптограф О. Керкхоффс, автор двух статей, опубликованных в 1883 году под общим названием «Военная криптография», отмечал, что криптографическая система должна быть защищенной, даже если известны все детали ее работы, кроме секретного ключа [1].

Целью данной работы является анализ теории и практики криптографической защиты и определение направлений ее развития на уровне публичных организаций и учреждений.

Современная криптология является разделом как математики, так и информатики; кроме того она также связана с инженерией, теорией информации и телеинформатической безопасностью. Ее принято разделять на:

а) криптографию, т. е. отрасль знаний о секретности сообщений;

б) криптоанализ - область знаний об эффективной атаке, то есть взломе защиты и расшифровке сообщений при отсутствии ключа или другого обязательного элемента схемы шифрования [2].

В настоящее время особенно актуальными являются криптографические защиты в процессе внедрения технологий электронного правительства, т. е.

оцифровывания сферы государственного управления и местного самоуправления, в управленческих процессах системы органов которых используется секретная информация, в том числе сведения о людях, обращающихся в эти публичные организации и учреждения.

При этом рекомендуется использовать такой инструмент криптографической защиты как секретные ключи, состоящие из нескольких десятков и даже сотен знаков, в процессе шифрования и дешифрования которых осуществляется миллионы операций.

На практике для того, чтобы найти определенный файл среди многих других, необходимо в первую очередь располагать его ярлыком (именем) - *англ. hash*. *Hash* - это серия букв и цифр с фиксированной длиной, которая в упрощенном виде называется «цифровой отпечаток» компьютерного файла. *Hash* может быть сгенерирован для любого типа файла, то есть текстовых файлов, изображений, звуков или фильмов.

Цель криптографии не в том, чтобы скрыть существование сообщения или факт общения между двумя сторонами, а в том, чтобы скрыть его значение. В этом преимущество криптографии перед стеганографией, потому что даже если сообщение перехвачено неавторизованным лицом, оно не может быть легко прочитано без знания процедуры шифрования и ключа.

Идея одновременного использования алгоритма и ключа возникает из возможности ограничения обмена информацией между заинтересованными сторонами. Информация о том, на сколько позиций вам нужно переместить буквы, имеет решающее значение в этом случае, в то время как информация о том, что вы собираетесь сдвинуться влево, сама по себе не угрожает секретности информации и для удобства может быть предоставлена в начале сообщения в незашифрованном виде.

Прочность шифра может быть определена путем оценки его устойчивости к атакам, осуществляемым только с технической стороны (т.е. без ошибок, вызванных лицом, использующим шифр). Обеспечение полной безопасности с помощью шифра - это самый высокий уровень безопасности, который можно

определить. На практике обычно используется термин «семантическая безопасность», который определяет условия для обеспечения практической безопасности шифра.

Шифр является семантически безопасным (англ. *semantically secure*), если знание зашифрованного текста и длины исходного сообщения не раскрывает никакой дополнительной и практически доступной информации об исходном тексте.

Идея шифрования основана на двух элементах: алгоритме шифрования и ключе. В специальной литературе отмечаются такие характеристики, которыми должен обладать криптографический алгоритм:

• математическая сложность алгоритма шифрования должна исключать возможность использования аналитических методов для взлома шифра;

• стоимость или время, необходимое для получения ключа или чтения простого текста из криптограммы, должно быть значительным и практически недопустимым.

Алгоритм шифрования должен удовлетворять вышеуказанным условиям, даже когда криптоаналитик имеет доступ к относительно большой части открытого текста и соответствующих криптограмм, а также когда он точно знает все детали алгоритма. Поэтому безопасность шифра не может опираться на секретность алгоритма шифрования, а зависит от секретности ключа, используемого для шифрования.

Термин «ключ» (англ. *key*) определяет в криптографии информацию, которая позволяет выполнять определенные криптографические действия, например, шифрование, дешифрование, подписывание информации, проверка подписи и т.п. [2].

Таким образом, практическое использование многочисленных инструментов криптогафической защиты предоставляет возможность обезопасить данные, используемые в различных сферах жизнедеятельности общества как на государственном, так и местном уровне, в том числе в публичных организациях и учреждениях.

Література:

1. Военная криптография [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki.

2. Schneier B. Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C / B. Schneier. – W-wa, 2002 – S. 27−28.