УДК 004.021

КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

К.С. ГОЛОВАН
(Представлено: Е.Р. СУХАРЕВ)

Раскрываются понятия целостности информации, контроля целостности информации и её актуальность. Приводятся методы контроля целостности информации: контрольные суммы, циклические коды, хэш-функции.

В условиях глубокого проникновения информационных технологий во все области жизнедеятельности человека надежность идентификации информации и контроль ее целостности становится важной проблемой, причем как научно-технической, так и социальной. Научно-техническая проблема включает в себя создание математических подходов, алгоритмов, программного и аппаратного обеспечения для решения этой проблемы. Социальный аспект проблемы связан с необходимостью создания общедоступной, удобной и защищенной системы надежной идентификации данных, адекватной степени развития информационных технологий.

Контроль целостности информации имеет огромное значение в различных областях деятельности человека. В финансовой области каждый день осуществляется большое количество финансовых транзакций в Интернете, в которых контроль целостности обрабатываемой, передаваемой и хранимой информации является важной частью.

Хозяйственная и юридическая деятельность также чрезвычайно критична к целостности информации в компьютерных сетях. В Беларуси в связи с утверждением «Инструкции о порядке взаимодействия ведомственных систем электронного документооборота с системой межведомственного электронного документооборота государственных органов» от 27 мая 2013 г. № 33 также возникает проблема контроля целостности сообщений и документов. Важность контроля целостности подтверждает принятие Закона Республики Беларусь от 28 декабря 2009 года № 113-З «Об электронном документе и электронной цифровой подписи».

Создание защищённой системы – задача комплексная, и решается она путём применения программно-технических средств, а также организационных мер. Реальная система защиты строится исходя из возможных угроз и выбранной политики безопасности.

Основными угрозами информационной безопасности по аспекту, на который эти угрозы направлены, являются:

- угрозы конфиденциальности;
- угрозы целостности;
- угрозы доступности;
- угрозы подлинности;
- угрозы сохранности.

Система защиты информации обеспечивает целостность информации, если она обеспечивает достоверность, полноту и защищённость информации от неумышленных и преднамеренных искажений при хранении, передаче и обработке.

Одним из способов обеспечения целостности информации является применение средств контроля целостности программного обеспечения и обрабатываемой информации, включая и её восстановление.

Контроль целостности информации программ и данных – обнаружение их любых несанкционированных изменений, которые могут носить как случайный характер, так и быть вызваны несанкционированными действиями.

Основной задачей средств контроля целостности информации является обеспечение такого состояния системы, когда невозможно скрыть факт любой несанкционированной модификации информации.

Защита информации от модификации требует решения комплекса задач, связанных с надёжность аппаратного и программного обеспечения, организационными вопросами, резервированием данных, защитой от компьютерных вирусов, проверкой целостности данных, оперативностью их восстановления и др. В реальных информационных системах всегда имеется существенная вероятность модифицирования информации. Одной из важнейших задач защиты от модифицирования данных является обнаружение факта искажения данных. Во многих случаях обнаружение этого факта является достаточно сложной задачей. Последствия от использования модифицированных программ и данных в информационных автоматизированных системах могут привести к большому ущербу.

Причинами нарушения целостности информации являются ненадёжность аппаратных средств, используемых в информационных технологиях, воздействие внешних электромагнитных излучений, наличие естественных помех в каналах связи, ошибки операторов и программистов, компьютерные вирусы и действия нарушителей. Многие из этих причин вызывают появление непреднамеренных ошибок, которые имеют случайный характер, а другие связаны с умышленными воздействиями на информацию.

Это может быть осуществлено специально внесённой в компьютерную систему программой или специально разработанным вирусом. Нарушитель, получая возможность несанкционированного доступа к информационным ресурсам, может внести изменения в электронные документы, модифицировать программу, удалить информацию из базы данных или внести дополнительную информацию. Умышленные воздействия имеют целенаправленный характер. При целенаправленном внесении изменений нарушитель может учитывать используемые механизмы обнаружения модификаций с целью осуществления такого модифицирования, которое нельзя было бы обнаружить. В некоторых случаях умышленные воздействия будут приводить к случайному модифицированию данных. Очевидно, что если решается задача обнаружения целенаправленного модифицирования, то одновременно решается задача обнаружения случайных искажений информации.

В общем случае контроль целостности информации реализуется путем предварительного определения характеристики целостности информации, называемой эталонной характеристикой, или эталонным кодом обнаружения модификаций. Эта эталонная характеристика по своему объему значительно меньше контролируемой информации, а ее значение отражает содержимое защищаемых от модификации данных. В зарубежной литературе эталонную характеристику обнаружения модификаций называют MAC-кодом (message authentication code) [3].

В процессе непосредственного контроля целостности информации выполняются следующие действия:

- для контролируемой информации определяется текущая характеристика обнаружения модификаций по тому алгоритму, по которому формировалась эталонная характеристика;
- текущая и эталонная характеристики обнаружения модификаций сравниваются. Если они совпадают, то считается, что контролируемая информация не подвергалась изменению.

К методам определения модификаций информации, вызванных случайным образом, относятся контрольное суммирование и использование циклических кодов.

Использование контрольных сумм и циклических кодов имеет существенный недостаток. Алгоритм получения контрольных характеристик для этих методов хорошо известен, поэтому злоумышленник может произвести модификации таким образом, чтобы контрольная характеристика не изменилась [3].

Задача злоумышленника значительно усложнится, если эталонная характеристика формируется и защищается криптографическими методами. Для этого необходимо использовать так называемую хэш-функцию. Преимущество хэш-функции в том, что она является необратимой функцией, т.е. для любого значения m легко вычислить $h(m)$, но для любого значения x невозможно найти такое m, что $h(m) = x$ [1].

В широком смысле термин «хэш-функция» используется для обозначения преобразований, которые отображают массив данных произвольного размера в блок данных фиксированного размера.

Функция хэширования позволяет осуществлять проверку целостности сообщений (документов), передаваемых в системах обработки информации различного назначения, с гарантированной достоверностью.

Для осуществления возможности контроля целостности данных необходимо вычислить от них значение функции хэширования и хранить его достоверным способом. При необходимости проверки целостности данных значение функции хэширования от этих данных вычисляется заново. В случае если вновь вычисленное значение совпало с достоверно хранимым, целостность данных подтверждается. В противном случае – целостность нарушена.

Функции хэширования применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур электронной цифровой подписи при передаче, обработке и хранении информации.

Хэш-функция должна удовлетворять следующим требованиям [2]:

- аргументом для хэш-функции может быть сообщение произвольной длины;
- значение хэш-функции имеет фиксированный размер;
- хэш-функция является эффективно вычислимой;
- хэш-функция является криптографически стойкой.

С точки зрения криптографической стойкости важным свойством хэш-функций является отсутствие коллизий, т.е. невозможно найти такие значения $x \neq y$, чтобы $h(x) = h(y)$. В криптографических приложениях важным понятием является криптографически стойкая хэш-функция, для которой не существует эффективного алгоритма нахождения значений $x \neq y$, где выполнялось бы условие $h(x) = h(y)$ (функ-

ция стойкая в сильном смысле), или не существует эффективного алгоритма нахождения коллизии при заданном x такого $y \neq x$ $h(x) = h(y)$ (функция стойкая в слабом смысле). Также было показано, что отсутствие коллизий не позволяет судить о практической стойкости хэш-функции. Практически значимым является отсутствие у хэш-функции корреляции. Свободной от корреляции называется хэш-функция, у которой невозможно найти пару $x \neq y$ такую, что вес Хэмминга двоичного вектора $h(x) \oplus h(y)$ будет меньше веса Хэмминга применительно к двоичному вектору $h(M)$ для некоторого малого M. Свобода от корреляции с точки зрения криптографической стойкости является гораздо более сильным свойством хэш-функции, чем свобода от коллизий [2].

Заключение. Угроза целостности является одной из основных угроз информационной безопасности. Несанкционированные изменения информации могут быть вызваны как случайными, так и преднамеренными действиями. Одним из способов обеспечения целостности информации является применение средств контроля целостности ПО и обрабатываемой информации, включая и её восстановление.

В общем случае контроль целостности информации реализуется путем предварительного определения характеристики целостности информации, называемой эталонной характеристикой, или эталонным кодом обнаружения модификаций.

В процессе непосредственного контроля информационной целостности выполняются следующие действия:

- для контролируемой информации определяется текущая характеристика обнаружения модификаций по тому алгоритму, по которому формировалась эталонная характеристика;
- текущая и эталонная характеристики обнаружения модификаций сравниваются. Если они совпадают, то считается, что контролируемая информация не подвергалась изменению.

Для выработки контрольных характеристик применяются криптографические хэш-функции.

ЛИТЕРАТУРА

1. Криптография: скоростные шифры / А.А. Молдовян [и др.]. – СПб. : БХВ-Петербург, 2002. – 496 с.
2. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян [и др.]. – СПб. : БХВ-Петербург, 2004. – 448 с.
3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты информации / А.А. Петров. – М. : ДМК, 2000. – 448 с.