УДК 519.72

Применение стохастических методов обеспечения безопасности и целостности информации

Рассмотрена проблема обеспечения достоверности и подлинности информации с применением стохастических методов. Использование стохастических преобразований не уменьшает стойкость безопасного преобразования и позволяет провести количественную оценку качественных параметров информации, таких как своевременность и ценность.

А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко

Вопросы обеспечения безопасности информации определяют развитие любой отрасли человеческой деятельности. Важным аспектом является предотвращение разглашения информации конфиденциального характера во время ее хранения, обработки или передачи. Надежным методом обеспечения безопасности информации можно считать преобразование данных с использованием определенных алгоритмов и последующую циркуляцию этих данных в неявном виде (с их восстановлением при необходимости). При построении алгоритмов подобного рода учитывается количественная оценка циркулирующей информации: длины передаваемых сообщений, их количество, скорость.

При рассмотрении качественной оценки информационной составляющей необходимо отметить, что количество информации (содержательной) невозможно рассматривать без учета ее полезности (ценности) и своевременности для пользователя, поэтому не менее важным аспектом является обеспечение достоверности и подлинности данных. Изменение вида и смысла данных может происходить из-за злоумышленных действий (дезинформация) или из-за воздействия помех, но в результате изменяется качественная составляющая информации, она становится менее ценной, менее своевременной и т. д. Применение качественных характеристик для описания позволяет объективно учитывать полезность получаемой информации, так как одинаковая информация может неоднозначно трактоваться для разных пользователей, различных ситуаций и собственных характеристик (информация кратковременного действия, долговременная информация и т. д.). Для анализа ценностного статуса необходимо рассматривать пользователя и его интересы как с субъективной точки зрения, учитывающей подготовку человека к восприятию и использованию информации определенного вида (если субъект не знает языка, на котором записано сообщение, для него ценность этого сообщения равна нулю), так и с объективной точки зрения, учитывающей значимость самого сообщения.

Достоинством применения качественных характеристик информации является возможность построения математических моделей систем (алгоритмов) обеспечения конфиденциальной и имитобезопасности на основе базовых алгоритмов.

В качестве базового примера математической модели, учитывающей ценностную составляющую информации, следует использовать трехосновную параметрическую функцию вида

$$A = <X, K, Y; f>, \quad (1)$$

где X, Y, K – конечные множества, состоящие из исходной, преобразованной информации и конфиденциальных параметров преобразования; f – функция преобразования, сюръективное отображение декартова произведения $X \times K$ в Y, т. е. $f: X \times K \to Y$.

В данной функции ценностная составляющая должна учитываться при определении любого элемента каждого множества. Например, при компрометации элемента $y \in Y$ можно определить множество $O(y) = \bigcup_{x \in X(y)} O(x)$ и выбрать $o^* \in O(y)$ в предположении $o^* = f(y)$. В этом случае ценность информации y будет определяться как

$$S(y) = C_{\alpha\beta}\left(\frac{1}{|O(y)|} - \frac{1}{|O|}\right), \quad (2)$$

где $C_{\alpha\beta} = \alpha - \beta$, при этом α – полученная прибыль в случае удачи ($o^* = f(y)$); β – потери в случае неудачи ($o^* \neq f(y)$). В надежной системе преобразования информации, не допускающей ее компрометации, $S(y) = 0$.

Следует отметить, что на параметры α и β влияют внешние факторы, вызывающие компрометацию $y \in Y$, а не структура, формирующая x и y.

Подобным образом можно учесть ценностную составляющую информации в любом элементе множеств X, Y, K.

С другой стороны, обеспечение имитобезопасности определяется возможностью успешного навязывания (дезинформация или воздействие помех) преобразованной информации $y \in Y$, соответствующей исходным данным $x \in X$. Тогда с учетом выбранных величин оценки α, β эффективность навязывания информации описывается величиной

$$Ef(x) = If(x)C_{\alpha\beta}\left(\frac{1}{|O(x)|} - \frac{1}{|O|}\right) - (1 - If(x))\frac{C_{\alpha\beta}}{|O|} = C_{\alpha\beta}\left(\frac{1}{|O(x)|} - \frac{1}{|O|}\right), x \in X, \quad (3)$$

где $If(x) = \begin{cases} 1, \text{ если } x \in X^+; \\ 0, \text{ если } x \notin X^+, \left(x \in X^-\right), x \in X. \end{cases}$

Подобная модель допускает использование аппарата восстановления данных в следующем виде: $y \in Y$ – исходное преобразованное сообщение, соответствующее исходным данным $x \in X$, $y' \in Y$ – измененное преобразованное сообщение, соответствующее навязываемым данным $x' \in X$, тогда потери от модификации данных могут быть оценены как

$$\Delta L = V(y) - V_L(y'/y), \quad (4)$$

где $V(y)$ – эффективность применения информации, принятой без модификации; $V_L(y'/y) = \frac{C_{\alpha\beta}}{|O(x)|} + \beta$ – эффективность применения модифицированной информации.

Соответственно при использовании алгоритмов восстановления информации выражение (4) будет модифицировано следующим образом:

$$\Delta L = V(y) - V_L(y'/y) + V_{K_V}(y'/y), \quad (5)$$

где $V_{K\gamma}(y'/y) = \dfrac{C_\gamma}{|O(y)|} + K_p$ – эффективность восстановления модифицированной информации; C_γ – коэффициент, учитывающий эффективность алгоритма восстановления $y' \to y$, K_p – поправочный коэффициент, учитывающий особенности формирования, преобразования, хранения, обработки информации.

Следует отметить, что в общем случае потери от навязывания не зависят от используемого вида преобразования, а зависят от эффективности системы (алгоритма) обнаружения и предотвращения модификации данных.

Принимая во внимание все вышесказанное, рассмотрение качественных характеристик информации необходимо проводить как составную часть процессов, обеспечивающих безопасность и целостность данных. Необходимо отметить, что механизмы обеспечения безопасности и целостности существенно отличаются как в теоретических, так и в практических постулатах. Например, устранение избыточности является неотъемлемым условием, используемым в алгоритмах преобразования данных для обеспечения безопасности информации, однако для надежной передачи, хранения и обработки данных с целью устранения их нежелательной модификации и возможности восстановления необходимо вводить избыточность в сообщения. Наличие подобных противоречий приводит к необходимости одновременного существования двух каналов (систем) обеспечения безопасности и целостности информации. Выходом из сложившейся ситуации является применение стохастических методов обеспечения безопасности и целостности информации, которые объединяют в себе оба этих механизма.

Применение стохастических методов обеспечения безопасности основано на построении помехоустойчивых кодов. Формируемый помехоустойчивый код содержит операции введения избыточности при кодировании и операции принятия решения о наличии модификации информации при декодировании, объединенные с операциями прямого и обратного стохастического преобразования.

Стохастическое преобразование представляет собой взаимосвязанную совокупность операций $ST(s, \gamma_k)$ над исходной последовательностью s длиной l и квазислучайной последовательностью γ_k длиной l или $2l$, имеющую обратную $ST^{-1}(e, \gamma_k)$ и обладающую свойствами симметричного канала, т. е. после обратного преобразования получается выражение

$$\begin{aligned} &ST^{-1}\left(ST\left(s, y_k\right) + u, y_k\right) = s + u; \\ &\text{при } u = 0 \;\; P(u = 0) = 1, \;\; P(u' \neq 0) = 0; \\ &\text{при } u \neq 0 \;\; P(u' = 0) = 0, \;\; P(u_j \neq 0) = (2^l - 1)^{-1} \;\; \text{для} \;\; j = \overline{0, (2^l - 1)}, \end{aligned} \tag{6}$$

где u и u' – исходный и преобразованный векторы ошибки, т. е. сумма по модулю 2 между искажаемым и искаженным векторами. Для обнаружения ошибок в данной системе (алгоритме) используется циклический (n, k)-код.

Искажение последовательности длиной $l = n$ при передаче по каналу связи вектором ошибки u в соответствии с некоторым распределением ошибок, описываемым вероятностями $P(e_i)$ для каждой $2^n - 1$ совокупности образцов ошибки u_i, причем преобразованные векторы ошибки будут описываться вероятностями

$$P\left(e_i'\right) = \begin{cases} 0 & \text{при } u = 0 \text{ для } i \in \left[1, 2^n - 1\right]; \; P\left(u_0\right) = 1, \\ 1/\left(2^n - 1\right) & \text{при } u \neq 0 \text{ для } i \in \left[1, 2^n - 1\right]; \; P\left(u_0\right) = 0. \end{cases} \tag{7}$$

Вероятность не обнаружения ошибки будет определяться ситуацией, когда после передачи некоторого кодового слова E_i циклического кода в декодер поступает комбинация E_j, также яв-

ляющаяся одним из кодовых слов, общее число которых равно 2^k. Такое событие происходит в том случае, если вектор ошибки e' является кодовым словом этого же кода. Так как число ненулевых кодовых слов в множестве $\{E\}$ равно $2^k - 1$, а число равновероятных ненулевых векторов ошибки e' равно $2^n - 1$, то после искажения необнаруженная ошибка происходит в $2^k - 1$ случаях из $2^n - 1$, т. е. условная вероятность необнаруженной ошибки в искаженном блоке равна

$$P(\varepsilon|u \neq 0) = \left(2^k - 1\right)\Big/\left(2^n - 1\right) \quad (8)$$

независимо от характера искажения, т. е. распределения e_i.

Причем вероятность необнаруженной ошибки не зависит от свойств (n, k)-кода, а зависит только от числа избыточных символов.

Обобщая все вышесказанное, можно выделить основные аспекты применения стохастического преобразования для описания качественных характеристик информации:

– использование стохастического преобразования не уменьшает стойкость безопасного преобразования за счет выполнения двух основных постулатов: равновероятности преобразованных сообщений и сопоставимости длин сообщения и конфиденциальных параметров, что не дает возможности использования полного перебора по всему пространству конфиденциальных параметров;

– использование стохастического преобразования позволяет обнаруживать ошибки и модификации информации, что позволяет сохранить качественные характеристики циркулирующей в системе информации и позволяет провести количественную оценку качественных параметров информации, таких как своевременность и ценность.

Список литературы

1. Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963.
2. Мазур М. Качественная теория информации. М.: Мир, 1974.
3. Стратонович Р. Л. О ценности информации. Изв. АН СССР. Технич. кибернетика. 1965, № 5. С. 3–13.
4. Гаврурин М. К. О ценности информации. Вестник ЛГУ. Сер. Матем., мех. и астрон. 1963. Вып. 4, № 19. С. 27–35.
5. Жуков И. Ю., Иванов М. А., Осмоловский С. А. Принципы построения генераторов псевдослучайных кодов, используемых при построении стойких криптоалгоритмов // Проблемы информационной безопасности. Компьютерные системы. 2001, № 1. С. 34–41.
6. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1971.
7. Вольфовиц Дж. Теоремы кодирования теории информации. М.: Мир, 1987.
8. Осмоловский С. А. О реализации стохастических кодов, исправляющих ошибки // Техника средств связи. Сер. ТПС. 1984. Вып. 6. С. 86–96.
9. Осмоловский С. А. О возможной реализации абсолютной секретности в постановке Шеннона // Системы и средства связи, телевидения и радиовещания. 2001, № 1. С. 15–22.

Implementation of Stochastic Methods, Underlying Information Safety and Integrity

A. P. Martynov, D. B. Nikolayev, V. N. Fomchenko

The problem of reliability and authenticity of information using stochastic methods is analyzed. Stochastic transformations do not reduce stability of safe conversion and provide for quantitative estimation of such qualitative parameters of information as timeliness and validity.