УДК 621.3.06

ОПТИМИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ОТНОСИТЕЛЬНО УСЛОВИЙ ТЕОРЕТИЧЕСКОЙ НЕДЕШИФРУЕМОСТИ

В.В. КОТЕНКО, С.В. КОТЕНКО, К.Е. РУМЯНЦЕВ, И.Д. ГОРБЕНКО

Приводится фундаментальное решение задачи оптимизации процессов защиты информации с позиций виртуализации относительно условий теоретической недешифруемости. Применение предложенного подхода открывает принципиально новую область возможностей для комплексного решения проблем повышения стойкости защиты информации.

Ключевые слова: ансамбль ключевых данных, комплексное решения проблем повышения стойкости, оптимизация процессов защиты информации, условия теоретической недешифруемости, энтропия ансамбля ключа.

ВВЕДЕНИЕ

До настоящего времени стратегия обеспечения теоретической недешифруемости (ТНДШ) информации по ряду причин считается практически нереализуемой. Этим во многом объясняется общепринятое отношение к ней как к некоему недостижимому ориентиру, не заслуживающему внимания в практических приложениях. Возможность решения этой проблемы открывает применение подхода, состоящего в виртуализации процессов защиты информации [1, 2, 3, 4]. Виртуализация, согласно отмеченного подхода, – это реализация возможного в установленных условиях при отсутствии ограничений на выбор условий.

1. ВИРТУАЛИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Следуя предложенной в [1, 2] методике виртуализации, установим основное условие теоретической недешифруемости и определим теоретические основы защиты дискретной информации (шифрования) для установленного условия.

Условие 1.1. Защита дискретной информации при определенной статистической зависимости сообщений и ключей должна сопровождаться соответствующим увеличением средней неопределенности ключей.

Теорема 1.1. Пусть шифрование Ф определяется ансамблями сообщений U^*, ключей K^* и криптограмм E^*. Тогда, если при шифровании Ф формирование криптограмм сопровождается увеличением средней неопределенности ключей при их статистической зависимости от сообщений, причем

$$H[K^*/U^*E^*] - H[K^*/U^*] = I[U^*;E^*], \quad (1)$$

то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Доказательство. Запишем выражение для среднего количества взаимной информации в виде

$$I[U^*K^*;E^*] = I[U^*;E^*] + I[K^*;\ U^*/E^*], \quad (2)$$

где

$$I[K^*;\ U^*/E^*] = I[K^*;U^*E^*] - I[K^*;U^*] = H[K^*/U^*E^*] - H[K^*/U^*]. \quad (3)$$

Из теоремы шифрования следует, что существование теоретически недешифруемого шифра Φ_0 возможно тогда, когда среднее количество взаимной информации $I[U^*K^*;E^*]$ будет равно нулю. Исходя из этого, на основании (2), с учетом (3) имеем

$$I[U^*;E^*] - (H[K^*/U^*E^*] - H[K^*/U^*]) = 0.$$

Откуда окончательно получаем

$$I[U^*K^*;E^*] = I[U^*;E^*] + I[K^*;\ U^*/E^*]. \quad (4)$$

Что и требовалось доказать.

Правую часть выражения (4) в приведенном доказательстве можно трактовать как изменение условной энтропии ключа при формировании криптограмм. Таким образом, из (4) и (1) следует довольно неординарный вывод о том, что теоретическая недешифруемость возможна и при статической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование сопровождается изменением условной энтропии ключа и если данное изменение будет компенсировать среднее количество взаимной информации о сообщениях в криптограммах. Неординарность этого вывода состоит в том, что он расширяет границы общепринятого *классического представления теоретической недешифруемости*, устанавливающего обязательную статистическую независимость сообщений и ключей от криптограмм, т. е.

$$H[U^*/E^*] = H[U^*] \quad (5)$$

$$H[K^*/E^*] = H[K^*] \quad (6)$$

откуда

$$I[U^*;E^*] = H[U^*] - H[U^*/E^*] = 0, \quad (5)$$

$$I[K^*;E^*] = H[K^*] - H[K^*/E^*] = 0. \quad (6)$$

Физический смысл этих условий вполне понятен. Он состоит в исключении какой-либо информации о сообщениях и ключах из криптограмм, формируемых при шифровании. Кроме

того, в основной массе практических приложений обычно постулируется статистическая независимость сообщений и ключей, что объясняется, по-видимому, стремлением обеспечить дополнительные гарантии теоретической недешифруемости. Это стремление, а также попытки максимально приблизиться к (5)–(8), на практике не только приводит к достаточно громоздким и неоптимальным решениям, но и существенно усложняет решение такой важной задачи, как обеспечение имитостойкости.

Теорема1 объясняет возможность существования теоретически недешифруемых шифров при статистической зависимости сообщений и криптограмм, когда равенства (5)–(8) не выполняются. При этом изначально допускается, что ансамбли U^* и K^* статистически связаны и отсутствие этой статистической зависимости рассматривается лишь как частный случай, при котором (1) принимает вид

$$H[K^*/E^*] - H[K^*] = I[U^*;E^*]. \qquad (7)$$

Откуда с учетом того, что

$$I[K^*;E^*] = H[K^*] - H[K^*/E^*] \qquad (8)$$

следует

$$I[K^*;E^*] = -I[U^*;E^*]. \qquad (9)$$

В свою очередь, если в выражении (1) учесть, что

$$H[K^*/U^*] - H[K^*/U^*E^*] = I[K^*;U^*/E^*] \qquad (10)$$

и в соответствии с этим привести его к виду

$$-I[K^*;U^*/E^*] = I[U^*;E^*], \qquad (11)$$

то становится понятным и общий физический смысл Теоремы 1. Оказывается, что теоретически недешифруемые шифры могут существовать и при статистической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование предполагает увеличение средней условной неопределенности ключей. Причем это увеличение должно обеспечиваться введением ложной информации о сообщениях в формируемые криптограммы.

Из доказанной теоремы следует принципиально новый подход к решению задач защиты дискретной информации, состоящий в допущении возможности существования теоретически недешифруемых шифров при статистической зависимости ансамблей сообщений, криптограмм и ключей. Введение регулируемой неопределенности изменения энтропии ансамбля ключа, соответствующей среднему количеству взаимной информации $I[U^*; E^*]$ в процессе шифрования, можно трактовать как виртуализацию алгоритма формирования ключей относительно условия 1.

Таким образом, установленное условие 1 и доказанная применительно к этому условию теорема 1 определяют обобщенную модель виртуализации защиты дискретной информации с позиций теоретической недешифруемости (рис. 1).

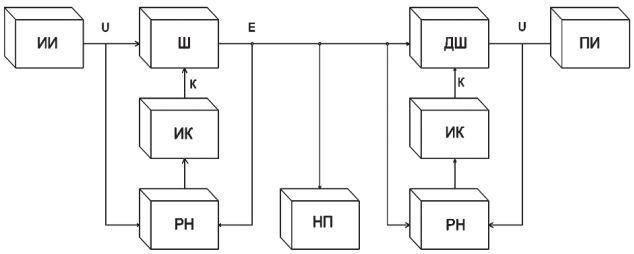

Рис. 1. Обобщенная модель виртуализации процесса защиты дискретной информации с позиций условий теоретической недешифруемости

Особенностью полученной модели является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности (РН) состояний источника ключа (ИК) по правилам, базирующимся на теоретической основе, установленной Теоремой1.

2. ВИРТУАЛИЗАЦИЯ ПРОЦЕССОВ ЗАЩИТЫ НЕПРЕРЫВНОЙ ИНФОРМАЦИИ

Виртуализация процесса защиты непрерывной информации заключается в установлении условий виртуализации, оптимизирующих этот процесс, и определении решений, соответствующих данным условиям.

В общем виде процесс защиты непрерывной информации представляет собой процесс преобразования непрерывных сообщений в криптограммы по секретному закону, определенному ключом. Обычно этот процесс называют *скремблированием*, а обратный ему процесс преобразования криптограмм в сообщения — *дескремблированием*. В зависимости от вида ансамбля формируемых криптограмм существует *два* основных варианта защиты непрерывной информации:

– аналоговое скремблирование, когда ансамбль формируемых криптограмм является непрерывным;

– цифровое скремблирование, когда ансамбль формируемых криптограмм дискретный.

Отличительной особенностью процесса защиты непрерывной информации является высокая избыточность непрерывных сообщений, которую, как правило, не удается в полной мере устранить в формируемых криптограммах. Решение этой проблемы определяет целесообразность виртуализации источников непрерывной информации относительно условий, устанавливающих достижение минимально возможного значения избыточности сообщений. При этом, возможно два варианта виртуализации источников непрерывной информации:

– виртуализация непрерывного источника при условии реализации виртуального непрерывного источника с минимально возможной избыточностью;

– виртуализация непрерывного источника при условии реализации виртуального дискретного источника с минимально возможной избыточностью.

Первый вариант виртуализации источников непрерывной информации применяется при аналоговом скремблировании, второй – при цифровом скремблировании. Исходя из этого, обобщенная модель процесса защиты непрерывной информации имеет два вида представления:

1) представление для аналогового скремблирования (рис. 2);

2) представление для цифрового скремблирования (рис. 3).

При аналоговом скремблировании непрерывные сообщения s(t) источника информации (ИИ) обычно подвергаются компандированию. Чаще всего это частотная компрессия непрерывных сообщений на выходе ИИ, означающая сжатие частотного диапазона спектра случайного процесса, представляющего ансамбль S источника. Формируемый таким образом процесс можно представить, как выборочное пространство некоторого *виртуального непрерывного источника* $\hat{S}$, обладающего меньшей избыточностью. Преобразование непрерывного ансамбля S в непрерывный ансамбль $\hat{S}$, применительно к условию минимизации избыточности, определяется как *непрерывная виртуализация источника*. Сообщения $s(t)$ этого источника путем преобразований аналогового скремблирования (ПАС) по закону, заданному элементами дискретного ансамбля K источника ключа (ИК), преобразуются в криптограммы $e(t)$ ансамбля криптограмм E. Ансамбль криптограмм в данном случае является непрерывным.

При дескремблировании производятся обратные преобразования аналогового скремблирования (ОПАС) криптограмм в сообщения $s(t)$, которые после экспандирования (декомпрессии) поступают к получателю информации. Закон обратных преобразований аналогового скремблирования задается ключами ансамбля K. При этом к криптограммам может получать доступ несанкционированный пользователь (НП). Основная задача защиты непрерывной информации в данном случае состоит в установлении аналогового скремблирования источника, обеспечивающего невозможность дескремблирования криптограмм при несанкционированном доступе к ним.

Нетрудно заметить, что основу решения данной задачи составляет выбор методов преобразований аналогового скремблирования. К используемым для этих целей методам ПАС принято относить: 1) методы коммутируемой инверсии; 2) методы частотных перестановок; 3) методы временных перестановок; 4) методы амплитудного скремблирования. Часто в целях повышения эффективности аналогового скремблирования применяют различные комбинации отмеченных методов в виде так называемых комбинированных методов ПАС. Однако, как показала практика, все это не позволяет обеспечить решение отмеченной основной задачи. Исходной причиной данной проблемы является высокая избыточность непрерывных сообщений, которую не удается устранить при формировании криптограмм. Так, например, для речевых сообщений характерна почти двадцатикратная избыточность, которая в значительной мере сохраняется и после скремблирования. Следствием этого является принятая в настоящее время *стратегия аналогового скремблирования*, основными направлениями которой выступают:

1) обеспечение временной стойкости защиты информации;

2) выполнение условий однозначности дескремблирования.

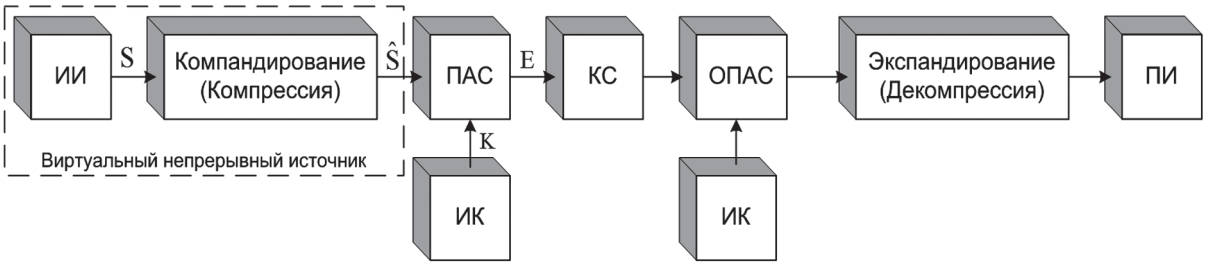

Рис. 2. Обобщенная модель аналогового скремблирования с позиций условия реализации виртуального непрерывного источника

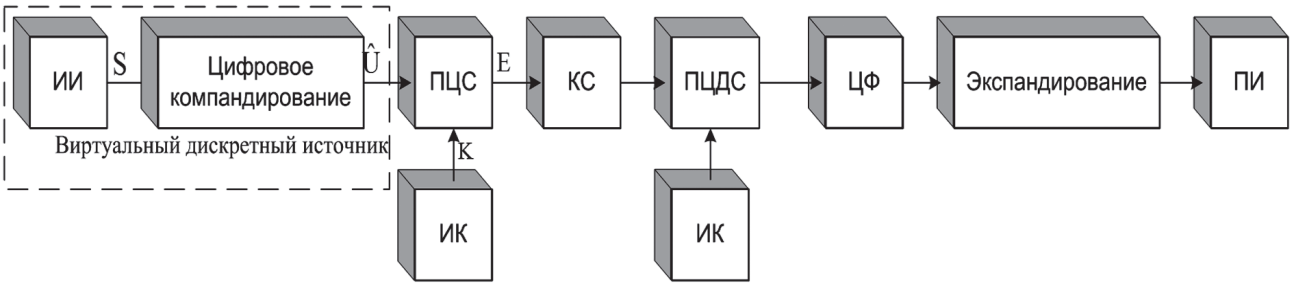

Рис. 3. Обобщенная модель цифрового скремблирования с позиций условия реализации виртуального дискретного источника

Условия однозначного дескремблирования обеспечиваются идентичностью ключевых последовательностей, используемых при скремблировании и дескремблировании, а также полной идентичностью прямых и обратных частотно-временных преобразований.

Цифровое скремблирование, в отличие от аналогового, обеспечивает более эффективное решение проблемы высокой избыточности непрерывных источников. Это достигается путем цифрового компандирования непрерывных сообщений $s(t)$ источника информации (ИИ). Полученные таким образом кодовые последовательности можно рассматривать, как элементы ансамбля $\hat{U}$, соответствующего некоторому *виртуальному дискретному источнику*. Преобразование непрерывного ансамбля S в дискретный ансамбль $\hat{U}$, применительно к условию минимизации избыточности, определяется как *дискретная виртуализация источника*. С этих позиций последующие преобразования цифрового скремблирования (ПЦС) и цифрового дескремблирования (ПЦДС) выступают аналогами шифрования и дешифрования при защите дискретной информации. Это во многом объясняет преимущественное применение в задачах цифрового скремблирования подходов, используемых при шифровании. При этом требуется учитывать *особенности, свойственные цифровому скремблированию*. Во-первых, на эффективность цифрового скремблирования существенное влияние могут оказывать потери информации, вызванные цифровым представлением. Во-вторых, применение в нем компандирования открывает дополнительные возможности для повышения качества защиты информации. Первая особенность обычно учитывается путем оптимальной цифровой фильтрации (ЦФ) результатов дескремблирования, вторая – путем подбора методов компрессии и экспандирования, обеспечивающих максимальное уменьшение избыточности для заданной точности восстановления непрерывной информации у получателя (ПИ).

Таким образом, принятая в настоящее время *стратегия цифрового скремблирования* включает следующие основные направления:

1) обеспечение гарантированной стойкости защиты информации;

2) выполнение условий однозначности дескремблирования;

3) обеспечение требуемой точности восстановления сообщений.

Следует обратить внимание, что данная стратегия, за исключением третьего направления, аналогична принятой в настоящее время стратегии защиты дискретной информации. Таким образом, цифровому скремблированию в принципе свойственны те же проблемы, что и шифрованию. Однако особенности цифрового скремблирования в значительной мере усиливают эти проблемы, требуя специфичных подходов к решению о*сновной задачи* защиты информации, состоящей в данном случае в установлении цифрового скремблирования, обеспечивающего невозможность дескремблирования криптограмм при несанкционированном доступе к ним. Прежде всего, это относится к проблеме абсолютной недешифруемости, которая при цифровом скремблировании приобретает специфику. Следует отметить, что при аналоговом скремблировании эта специфика значительно усиливается, делая решение проблемы абсолютной недешифруемости практически невозможным.

С позиций теории виртуализации стратегия решения проблемы абсолютной недешифруемости защиты непрерывной информации определяется как:

– установление условий виртуализации непрерывных источников информации;

– установление условий теоретической недешифруемости защиты непрерывной информации;

– установление условий, при которых любой продуктивный прогноз ключа является невозможным;

– определение теоретических основ защиты непрерывной информации (скремблирования) в установленных (заданных) условиях.

Согласно принятой стратегии, установим основные условия теоретической недешифруемости и определим теоретические основы защиты непрерывной информации (скремблирования) для установленных условий. По аналогии с шифрованием основу определения условий обеспечения абсолютной недешифруемости при защите непрерывной информации составляет определение теорем скремблирования.

Теорема 2.1. Теорема аналогового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений S, непрерывным ансамблем криптограмм E и дискретным ансамблем ключей K. Тогда, если среднее количество взаимной информации равно

$$I[SK;E] = 0, \qquad (12)$$

то существует аналоговое скремблирование Φ_{CA}, обеспечивающее теоретическую недешифруемость.

Доказательство. Теоретическая недешифруемость дескремблирования криптограмм при несанкционированном доступе означает, что

$$J[s_i(t)k(i);e_i(t)] = 0 \text{ , для всех } i \text{ ,}$$

т. е. количество информации о сообщении $s_i(t)$ и соответствующем ему i -м ключе $k(i)$, содержащееся в криптограмме $e_i(t)$, должно быть равным нулю.

Среднее количество взаимной информации о сообщениях и ключах в криптограммах определяется как

$$I[SK;E]=M\left[J[s_i(t)k(i);e_i(t)]\right], \qquad (13)$$

где $M\left[J[s_i(t)k(i);e_i(t)]\right]$ – функция математического ожидания.

Так как количество информации всегда неотрицательная величина, т. е. $J[s_i(t)k(i);e_i(t)] \geq 0$, то равенство (12) всегда будет однозначно свидетельствовать о выполнении (13). Что и требовалось доказать.

Криптограммы при аналоговом скремблировании с физической точки зрения можно рассматривать как результат искажения непрерывных сообщений источника некоторым гипотетическим непрерывным шумом скремблирования, характеристики которого определяются элементами дискретного ансамбля ключа. Исходя из этого, доказанная теорема позволяет определить условия, при которых исключается возможность дескремблирования криптограмм при несанкционированном доступе, т. е. когда среднее количество информации о сообщениях в криптограммах будет стремиться к нулю.

Теорема 2.2. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, непрерывным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть s_i и e_i – случайные величины, представляющие выборки реализаций непрерывных выборочных пространств ансамблей сообщений и криптограмм, соответственно, и пусть σ_i^2 – дисперсия искажающего воздействия на сообщение в процессе скремблирования, заданного составляющими выборочного пространства ансамбля ключа. Тогда среднее количество информации о сообщениях в криптограммах при аналоговом скремблировании будет стремиться к нулю, если дисперсия σ_i^2 будет стремиться к бесконечности, т. е. $\sigma_i^2 \to \infty$.

Доказательство. Введем ряд упрощений, не влияющих на общность доказательства. Будем считать, что сообщения источника имеют гауссовский закон распределения, а также, что сообщения и криптограммы статистически не связаны с элементами дискретного ансамбля ключа. Таким образом, с учетом гауссовской аппроксимации сообщения можно представить как гауссовскую случайную величину с нулевым средним значением, дисперсией σ_s^2 и плотностью вероятности вида:

$$P(s_i) = \frac{1}{\sqrt{2\pi\sigma_s^2}} \exp\left(-\frac{s_i^2}{2\sigma_s^2}\right). \qquad (14)$$

Исходя из статистической независимости сообщений и криптограмм от элементов дискретного ансамбля ключа, искажающее воздействие на сообщение в процессе скремблирования, можно считать аддитивным вид гауссовской случайной величины с нулевым средним значением и дисперсией σ_i^2. Тогда условная плотность вероятности криптограмм при условии, что заданы сообщения, имеет вид

$$P(e_i / s_i) = \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left[-\frac{(e_i - s_i)^2}{2\sigma_i^2}\right]. \qquad (15)$$

Так как криптограммы в данном случае представляются как сумма двух гауссовских случайных величин, их также можно считать гауссовской случайной величиной с дисперсией $\sigma_s^2 + \sigma_i^2$ и плотностью вероятности

$$P(e_i) = \frac{1}{\sqrt{2\pi(\sigma_s^2 + \sigma_i^2)}} \exp\left[-\frac{e_i^2}{2(\sigma_s^2 + \sigma_i^2)}\right].$$

Выражения (14) и (15) позволяют определить дифференциальную условную энтропию для ансамблей *S* и *E*:

$$h[E/S] = -\int P(s_i) \int P(e_i / s_i) \log P(e_i / s_i)\, de_i ds_i =$$

$$= \int P(s_i) \int P(e_i / s_i) \left[\log\sqrt{2\pi\sigma_i^2} + \frac{(e_i - s_i)^2}{2\sigma_i^2} - \log e\right] de_i ds_i.$$

Учитывая, что $\int P(e_i / s_i)\left(e_i^2 - s_i^2\right) de_i$ равен дисперсии условного распределения σ_i^2, получаем

$$h[E/S] = \int P(s_i)\left[\log\sqrt{2\pi\sigma_i^2} + \frac{1}{2}\log e\right] ds_i =$$

$$= \frac{1}{2}\log\left(2\pi e\sigma_i^2\right).$$

Аналогично можно определить выражение для дифференциальной энтропии криптограмм:

$$h[E] = \frac{1}{2}\log\left[2\pi e\left(\sigma_s^2 + \sigma_i^2\right)\right].$$

Откуда окончательно получаем выражение для средней взаимной информации:

$$I[S;E] = h[E] - h[E/S] = \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_i^2}\right). \qquad (16)$$

Из (16) следует, что среднее количество информации о сообщениях в криптограммах стремится к нулю, когда дисперсия σ_i^2 стремится к бесконечности. Что и требовалось доказать.

Полученный результат может быть обобщен для случая, когда выборочные пространства сообщений и криптограмм задаются случайными процессами. С учетом этого доказанная теорема имеет принципиально важное практическое значение. Она *показывает невозможность обеспечения условий ТНДШ при аналоговом скремблировании* и во многом объясняет непродуктивность поиска подходов, практически исключающих возможность дескремблирования криптограмм при несанкционированном доступе.

Теорема 2.3. Теорема цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, дискретным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля *S*. Тогда, если среднее количество взаимной информации равно

$$I[\hat{U}\,K;E] = 0,$$

то всегда существует цифровое скремблирование Φ_{CD}, обеспечивающее теоретическую недешифруемость.

Доказательство. Теоретическая недешифруемость дескремблирования криптограмм при несанкционированном доступе для рассматриваемого случая означает, что

$$J[u(i)k(i);e(i)]=0, \qquad (17)$$

т. е. количество информации о сообщении $s_i(t)$, представленное в $u(i)$, и ключе $k(i)$, содержащееся в криптограмме $e(i)$, должно быть равным нулю.

Среднее количество взаимной информации о сообщениях и ключах в криптограммах для рассматриваемого случая определяется как

$$I[UK;E]=M\left[J[u(i)k(i);e(i)]\right], \qquad (18)$$

где $M\left[J[u(i)k(i);e(i)]\right]$ — функция математического ожидания.

Так как количество информации всегда неотрицательная величина, т. е. $J[u(i)k(i);e(i)]\geq 0$, то равенство (17) всегда будет однозначно свидетельствовать о выполнении (18). Что и требовалось доказать.

Теорема 2.4. Теорема виртуализации цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений *S*, дискретным ансамблем криптограмм *E* и дискретным ансамблем ключей *K*. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля *S*. Пусть элементы выборочного пространства ансамбля $\hat{U}$ формируются в результате цифрового компандирования сообщений выборочного пространства ансамбля *S*. Тогда, если при цифровом скремблировании, заданном дискретными ансамблями ключей *K* и криптограмм *E*, средняя взаимная информация $I[\hat{U}\,K;E]=0$, то всегда и только всегда будет справедливо равенство $I[SK;E]=0$.

Доказательство. Как уже отмечалось, к особенности цифрового скремблирования относится то, что преобразованиям цифрового скремблирования подвергаются не сами непрерывные сообщения ансамбля *S* источника, а результаты их цифрового компандирования, составляющие ансамбль $\hat{U}$. Исходя из этого, выражение для средней взаимной информации $I[S\,K;\,E]$ может быть представлено в виде

$$I[SK;E]=I\left[S\hat{U}\,K;E\right]=$$
$$=I\left[\hat{U};E\right]+I\left[K;E/\hat{U}\right]+I\left[S;E/K\hat{U}\right].$$

Отметим, что сумма двух первых членов правой части соответствует средней взаимной информации $I[\hat{U}\,K;E]=0$. Исходя из этого, выражение может быть приведено к виду

$$I[SK;E]=I\left[\hat{U}\,K;E\right]+I\left[S;E/K\hat{U}\right]. \qquad (12)$$

Запишем выражение для второго члена правой части:

$$I\left[S;E/K\hat{U}\right]=I\left[S;K\hat{U}\,E\right]-I\left[S;K\hat{U}\right]. \qquad (13)$$

Вследствие отмеченной особенности цифрового скремблирования средняя взаимная информация о сообщениях ансамбля *S* источника в элементах ансамблей $\hat{U}$, *K* и *E* будет однозначно определяться средней взаимной информацией о сообщениях ансамбля *S* в результатах их цифрового компандирования, составляющих ансамбль $\hat{U}$, т. е.

$$I\left[S;K\hat{U}\,E\right]=I\left[S;K\hat{U}\right]=I\left[S;\hat{U}\right].$$

Откуда окончательно получаем

$$I[SK;E]=I\left[\hat{U}\,K;E\right]. \qquad (19)$$

Таким образом, для выполнения равенства $I[SK;E]=0$ необходимо и достаточно выполнение равенства $I[\hat{U}\,K;E]=0$. Что и требовалось доказать.

Доказательство теоремы устанавливают взаимосвязь цифрового скремблирования и шифрования. Так, выражение (19) дает основание считать, что условия теоретической недешифруемости защиты дискретной информации, применимые для виртуального дискретного ансамбля сообщений $\hat{U}$, будут применимы и для соответствующего ему исходного непрерывного ансамбля *S*. При этом теоремы 2.1 – 2.4 и будут определять теоретические основы реализации этих условий и, как следствие, обобщенную модель виртуализации защиты непрерывной информации с позиций условий теоретической недешифруемости (рис. 4).

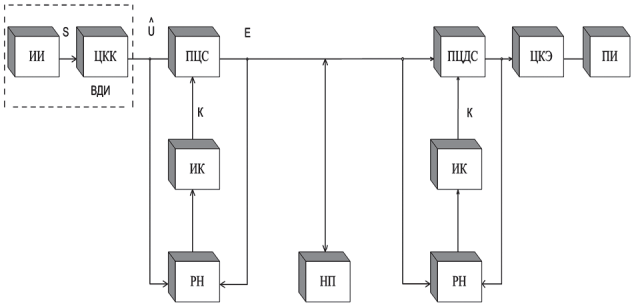

Рис. 4. Обобщенная модель виртуализации процесса защиты непрерывной информации с позиций условий теоретической недешифруемости

Особенностью полученной модели является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности (РН) состояний источника ключа. Ансамбль $\hat{U}$ является результатом виртуализации ансамбля *S* непрерывного источника информации. Таким образом, эффективность обобщенной модели процесса защиты непрерывной информации, с позиций условий теоретической недешифруемости (рис. 4), зависит от

установленных условий виртуализации непрерывного источника информации.

Основу виртуализации непрерывных источников при цифровом скремблировании составляет цифровое компандирование, предусматривающее компрессию (ЦКК) при скремблировании и экспандирование (ЦКЭ) при дескремблировании (рис. 4). С этих позиций к основным *условиям виртуализации непрерывных источников при цифровом скремблировании* относятся:

1. Минимизация информационных потерь.

2. Обеспечение минимальной избыточности.

Обеспечение установленных условий целесообразно рассматривать относительно к цифровому скремблированию, т. к. из доказательства теоремы 2.2 следует невозможность обеспечения условий ТНДШ при аналоговом скремблировании. Поэтому виртуализация непрерывных источников при цифровом скремблировании определяется как цифровая виртуализация.

ВЫВОДЫ

1. При теоретически недешифруемой защите дискретной информации ансамбль ключевых данных не оказывает влияния на стойкость шифрования, что позволяет использовать ключевые данные, открытые для несанкционированного доступа.

2. Защита дискретной информации при определенной статистической зависимости сообщений и ключей должна сопровождаться соответствующим увеличением средней неопределенности ключей.

3. Теоретическая недешифруемость возможна при статической зависимости ансамблей сообщений и криптограмм, если шифрование сопровождается изменением условной энтропии ключа и если данное изменение будет соответствовать среднему количеству взаимной информации о сообщениях в криптограммах.

4. Теоретически недешифруемая защита дискретной информации может обеспечиваться при статистической зависимости ансамблей сообщений, ключей и криптограмм, если предполагается увеличение средней условной неопределенности ключей. Причем это увеличение должно обеспечиваться введением ложной информации о сообщениях в формируемые криптограммы.

5. Введение регулируемой неопределенности изменения энтропии ансамбля ключа, в процессе шифрования, можно трактовать как изменение алгоритма формирования ключей соответственно установленным условиям теоретической недешифруемости, т.е. как виртуализацию алгоритма формирования ключей.

6. При цифровом скремблировании условия теоретической недешифруемости защиты дискретной информации, применимые для виртуального дискретного ансамбля сообщений, будут применимы и для соответствующего ему исходного непрерывного ансамбля сообщений.

7. Особенностью обобщенной модели процесса защиты непрерывной информации с позиций условий теоретической недешифруемости является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности состояний источника ключа.

8. Непрерывное сообщение, полученное в результате цифрового дескремблирования (оценка) и ошибка цифрового компандирования должны быть независимыми.

Литература

[1] *Котенко В.В.* Теория информации и защита телекоммуникаций: монография / В.В. Котенко, К.Е. Румянцев. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.

[2] *Величкин А.И.* Передача аналоговых сообщений по цифровым каналам. – М.: Радио и связь. – 1983. – 240 с.

[3] *Kotenko V., Rumjantsev K., Kotenko S.* "New Approach to Evaluate the Effectiveness of the Audio Information Protection for Determining the Identity of Virtual Speech Images". Proc. of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery (ACM). New York. Publications Dept., ACM, Inc. 2009, pp. 235–239.

[4] *Котенко В.В.* Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177–183.

[5] *Котенко В.В.* Теоретические основы виртуализации представления объектов, явлений и процессов // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 32–48

[6] *Котенко В.В.* Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 69–80.

[7] *Котенко В.В.* Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа. // Информационное противодействие угрозам терроризма: науч.-практ. журн., 2011, № 17. – С. 96–104.

Поступила в редколлегию 19.03.2013

Котенко Владимир Владимирович, профессор кафедры информационной безопасности телекоммуникационных систем факультета информационной безопасности Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Котенко Станислав Владимирович, аспирант Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Румянцев Константин Евгеньевич, заведующий кафедрой информационно безопасности телекоммуникационных систем факультета информационной безопасности Южного федерального университета. Научные интересы: защита информации в информационно-телекомуникационных системах, информационное противодействие угрозам терроризма.

Горбенко Иван Дмитриевич, фото и сведения об авторе см. на стр. 201.

УДК 621.3.06

Оптимізація процесів захисту інформації з позицій віртуалізації щодо умов теоретичної недешифрувальності / В.В. Котенко, С.В. Котенко, К.Є. Румянцев, І.Д. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 265–272.

Наводиться фундаментальне розв'язання задачі оптимізації процесів захисту інформації з позицій віртуалізації щодо умов теоретичної недешифрувальності. Застосування запропонованого підходу відкриває принципово нову область можливостей для комплексного вирішення проблем підвищення стійкості захисту інформації.

Ключові слова: ансамбль ключових даних, комплексне вирішення проблем підвищення стійкості, оптимізація процесів захисту інформації, умови теоретичної недешифрувальності, ентропія ансамблю ключа.

Іл.: 4. Бібліогр.: 7 найм.

UDC 621.3.06

Optimization of information security processes in terms of virtualization relative to conditions of theoretical indecipherability / V.V. Kotenko, S.V. Kotenko, K.E. Rumyantsev, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 265–272.

The fundamental solution of the problem of optimization of information security processes from virtualization positions concerning conditions of theoretical indecipherability is provided. Application of the offered approach opens a brand new area of opportunities for the complex solution of problems of improving information security.

Keywords: ensemble of key data, complex solution of problems of improving security, optimization of processes of information security, conditions of theoretical indecipherability, entropy of a key ensemble.

Fig.: 4. Ref.: 7 items.