СИСТЕМЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 621.3.06

СТРАТЕГИЯ ЗАЩИТЫ НЕПРЕРЫВНОЙ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ АНСАМБЛЯ КЛЮЧЕЙ НА ФОРМАЛЬНЫЕ ОТНОШЕНИЯ АНСАМБЛЕЙ

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

Приводится фундаментальное обоснование стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей. Устанавливается, что применение стратегии впервые открывает возможность трехуровневой защиты непрерывной информации. Оценка эффективности защиты от криптоанализа на первом (начальном) уровне защиты показывает потенциальную возможность выполнения условий абсолютной недешифруемости путем соответствующего увеличения дисперсии ансамбля виртуальных ключей.

Ключевые слова: ансамбль ключей, виртуализация процесса защиты непрерывной информации, объём выборочного пространства ансамбля ключевых данных, трехуровневая защита непрерывной информации, энтропия виртуального ансамбля ключей.

ВВЕДЕНИЕ

Особенностью виртуализации процесса защиты непрерывной информации является возможность использования исходного ансамбля источника сообщений в качестве непрерывного ансамбля виртуализации [1]. Отображение модели защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей, следующее из условия реализации отмеченной возможности, приведено на рис. 1.

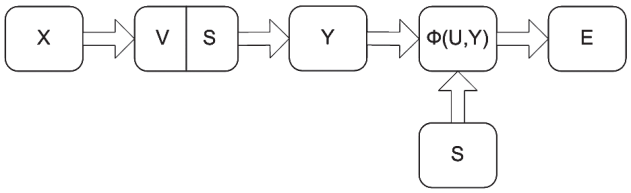

Рис. 1. Отображение модели защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей

Приведенное отображение показывает формальные функциональные отношения ансамблей, определяющих защиту непрерывной информации, при условии использования в качестве непрерывной составляющей ансамбля виртуализации исходного ансамбля источника сообщений *S*. Выборочное пространство ансамбля *V*, являющееся отображением ансамбля ключевых данных *X*, представляет дискретную составляющую ансамбля виртуализации *VS*. Дискретное выборочное пространство ансамбля *V* определяет функциональную форму изменения непрерывного выборочного пространства ансамбля *S*, которая отображается в дискретную форму выборочного пространства ансамбля ключевых последовательностей *Y*. Выборочное пространство ансамбля ключевых последовательностей *Y* используется для представления Φ_{CD} ансамбля сообщений виртуального дискретного источника $\hat{U}$, полученного в результате цифровой виртуализации непрерывного источника *S*, ансамблем криптограмм *E*.

Анализ отображения рис. 1 показывает, что разработка стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей невозможна без ответа на два основных вопроса:

1. Насколько включение исходного ансамбля сообщений *S* в состав ансамбля виртуализации способно влиять на стремление к бесконечности энтропии виртуального ансамбля ключей?
2. Какие ограничения на объём выборочного пространства ансамбля ключевых данных *X* накладывает включение в состав ансамбля виртуализации непрерывного ансамбля *S*?

1. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ

Теорема 1. Пусть скремблирование Φ_{CD} определяется ансамблем сообщений виртуального дискретного источника $\hat{U}^*$, ансамблем криптограмм E и виртуальным ансамблем ключей *K*, представленным совместным ансамблем *XYVZ*, где *VZ* – совместный дискретно-непрерывный ансамбль виртуализации. Тогда, если в совместный ансамбль виртуализации в качестве непрерывного ансамбля *Z* включить исходный ансамбль сообщений, то энтропия дискретно-непрерывного ансамбля виртуализации и энтропия виртуального ансамбля ключей будут стремиться к бесконечности, а вероятность продуктивного анализа ключа будет стремиться к нулю.

Доказательство. Энтропию дискретно-непрерывного ансамбля виртуализации согласно постановочной части теоремы можно представить как:

$$H[VZ] = H[VS] = H[S] + H[V/S]. \quad (1)$$

Из (1) следует, что при установленном стремлении абсолютной энтропии непрерывного ансамбля S к бесконечности, энтропия дискретно-непрерывного совместного ансамбля VS так же стремится к бесконечности.

Выражение для энтропии ансамбля ключей при включении в соответствующий ему совместный ансамбль непрерывного ансамбля S можно представить в виде:

$$H[K] = H[XYVS] = H[S] + H[XYV/S]. \quad (2)$$

Энтропия $H[S]$ в (2) представляет собой абсолютную энтропию непрерывного ансамбля, которая всегда стремится к бесконечности. Отсюда, согласно (2) энтропия виртуального ансамбля ключей $H[K]$ будет стремиться к бесконечности, а вероятность продуктивного анализа ключа будет стремиться к нулю. Что и требовалось доказать.

Теорема 2. Пусть скремблирование Φ_{CD} определяется ансамблем сообщений виртуального дискретного источника $\hat{U}^*$, ансамблем криптограмм E и виртуальным ансамблем ключей K, представленным совместным ансамблем $XYVZ$, где VZ – совместный дискретно-непрерывный ансамбль виртуализации. Тогда, включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля Z исходного ансамбля сообщений S не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных X.

Доказательство. Так как ансамбль S непрерывный, то формирование виртуальных выборочных пространств совместного ансамбля ключей $XVSY$ обеспечивает абсолютную недешифруемость. Пусть выборочное пространство ансамбля X содержит N точек. Тогда выражение для средней взаимной условной вероятности $I[XV;Y/S]$ можно представить двумя способами:

$$I[XV;Y/S] = I[X;Y/S] + I[V;Y/SX], \quad (3)$$

$$I[XV;Y/S] = I[X;Y/SV] + I[V;Y/S]. \quad (4)$$

Последнее слагаемое в (3) и последнее слагаемое в (4) неотрицательны и ограничены сверху величиной $\max H[V] \le \log_2 N_V$. Отсюда, приравнивая правые части в (66) и (67), можно получить

$$\left| I[X;Y/SV] - I[X;Y/S] \right| \le \log_2 N_V. \quad (5)$$

Статистическая независимость X и Y определяет справедливость равенства

$$I[X;Y/S] = 0. \quad (6)$$

С учётом (6), неравенство (5) принимает вид:

$$\log_2 N_V \ge I[X;Y/SV]. \quad (7)$$

Так как среднее количество информации всегда положительно, знак модуля при переходе от (5) к (7) опускается.

Запишем выражение для $I[X;Y/SV]$ в виде

$$I[X;Y/SV] = H[X/SV] - H[X/YSV], \quad (8)$$

где

$$H[X/YSV] = \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{1}{P(x/y,s,v)} ds =$$

$$= \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{P(x,y,s)}{P(x,y,s,v)} ds.$$

Применяя цепную формулу для вероятности, имеем

$$H[X/YSV] =$$

$$= \sum_x \sum_y \sum_v \int_s P(x,y,s,v) \log \frac{P(y/sv)}{P(x/sv)\, p(y/xsv)} ds, \quad (9)$$

откуда, учитывая статистическую независимость X и Y

$P(v) = P(y/sv)$ для всех x, y, s, v при $P(xsv) > 0$, получаем

$$H[X/YSV] = \sum_x \sum_v \int_s P(xsv) \log \frac{1}{P(x/sv)} ds =$$

$$= H[X/SV].$$

С учётом этого неравенство (7) основании (8) приводится к виду:

$$\log_2 N_V \ge 0. \quad (10)$$

Принимая во внимание, что выборочное пространство ансамбля V является однозначной дискретной проекцией выборочного пространства ансамбля ключевых данных X, можно записать:

$$\log N_V = \log N,$$

откуда с учетом (10) следует:

$$N \ge 1. \quad (11)$$

Из (11) следует, что минимально возможное число точек выборочного пространства ансамбля V^*, обеспечивающее абсолютную недешифруемость, равно 1. Это значение можно рассматривать как предел сжатия виртуальной дискретной проекции выборочного пространства ансамбля ключевых данных X. Учитывая однозначную взаимосвязь элементов этой проекции с ключевыми данными, этот предел может быть отнесен и к выборочному пространству ансамбля ключевых данных. Это означает, что при виртуализации ансамбля ключей путем включения в состав совместного ансамбля виртуализации исходного ансамбля сообщений S абсолютная недешифруемость сохраняется при сокращении (сжатии) множества исходных ключей до одного ключа. Это означает, что включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля Z исходного ансамбля сообщений S не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных X. Что и требовалось доказать.

2. ЭФФЕКТИВНОСТЬ СТРАТЕГИИ

На основании теорем 1–2 обобщенная модель реализации стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей может быть приведена к виду рис. 2.

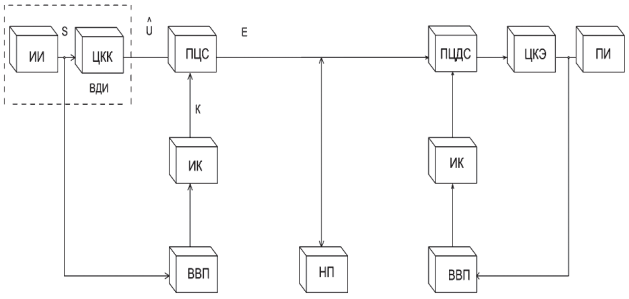

Рис. 2. Обобщенная модель реализации стратегии защиты непрерывной информации с позиций виртуализации ансамбля ключей на формальные отношения ансамблей

Нетрудно заметить, что полученная в [2] обобщенная схема адаптивного цифрового скремблирования является частным случаем реализации модели, приведенной на рис. 2.

Возможности обеспечения абсолютной недешифруемости, которые открывает реализация полученной модели (рис. 2), определяют актуальность поиска подходов к оценке стойкости и эффективности виртуального скремблирования, с позиций виртуализации ансамбля ключей. Проблема в данном случае состоит в специфике определения условной энтропии, определяющей стойкость защиты непрерывной информации $C\left(\Phi_{CD_X},S\right)$, входящей в состав выражения для эффективности защиты $D\left(\Phi_{CD_X},S\right)$:

$$D\left(\Phi_{CD_X},S\right)=D\left(\Phi_{CD_X},\hat{U}\right)=C\left(\Phi_{CD_X},\hat{U}\right)-H\left[Y_p\right],$$

$$C\left(\Phi_{CD_X},\hat{U}\right)=H\left[Y_p/E\right],$$

где Φ_{CD_X} – используемый шифр; U,E,Y_p – ансамбли сообщений, криптограмм и развернутых ключевых последовательностей, соответственно; X – ансамбль ключевых данных.

Условная энтропия $H[Y_p/E]$ характеризует среднюю неопределенность значения развернутого ключа $y_{i.}$ возникающую при несанкционированном перехвате соответствующего значения криптограммы $e_{i.}$. С физической точки зрения ее можно интерпретировать как среднее количество информации, которого не хватает для принятия однозначного правильного решения об y_i при криптоанализе $e_{i.}$. При этом особенностью виртуального скремблирования является то, что элементы дискретного ансамбля Y_p являются выборками реализаций $k_B(t)$ непрерывного выборочного пространства Z ансамбля виртуализации. Выборочное пространство Z, определяется дискретным выборочным пространством V ансамбля виртуализации, элементы которого, в свою очередь, однозначно определяются исходными ключами $k_И$ выборочного пространства ансамбля ключевых данных. Таким образом, криптоанализ виртуального скремблирования должен быть многоэтапным, включая:

– определение реализации виртуального ключа $k_B(t)$ по известным значениям криптограмм e_i;

– определение и вычисление значений параметров, задающих $k_B(t)$;

– определение исходного ключа по известным значениям задающих $k_B(t)$ параметров.

Последовательная реализация этих этапов в полном объеме являются необходимым условием успешного криптографического анализа при виртуализации процесса защиты непрерывной информации. В данном случае каждый этап может рассматриваться как уровень защиты. С этих позиций для успешного криптоанализа виртуального скремблирования необходимо преодолеть *трехуровневую защиту*, в отличие от одноуровневой, присущей для известных подходов. При этом значение $D_1\left(\Phi_{CD_X},S\right)$ и $C_1\left(\Phi_{CD_X},S\right)$ на первом уровне можно рассматривать как нижние границы диапазона изменения эффективности и стойкости виртуального скремблирования:

$$D_1\left(\Phi_{CD_X},S\right)=C_1\left(\Phi_{CD_X},S\right)-H[Y_p], \qquad (12)$$

$$C_1\left(\Phi_{CD_X},S\right)=H[\ \ _B/E]=$$

$$=\sum_i\int_{-\infty}^{\infty}p(e_i)P(k_{Bi}/e_i)\log\frac{1}{P(k_{Bi}/e_i)}dk_{Bi}. \qquad (13)$$

Здесь $P(k_{Bi}/e_i)$ является условной плотностью вероятности того, что при формировании значения e_i использовалось значение k_{Bi}. С позиций криптоанализа виртуального скремблирования, где на первом этапе стоит задача определения k_{Bi} по значениям e_i, виртуальный ключ можно рассматривать как результат искажения e_i некоторым гипотетическим случайным шумом, заданным процедурой скремблирования. С этих позиций задача криптоанализа сводится к оценке данного искажения. Если представить это искажение как аддитивное, то при гауссовской аппроксимации выражение для условной вероятности в (13) может быть определено как

$$P(k_{Bi}/e_i)=\frac{1}{\sqrt{2\pi\sigma_i^2}}\exp\left(-\frac{(k_{Bi}-e_i)^2}{\sigma_i^2}\right), \qquad (14)$$

где σ_i^2 — дисперсия условного распределения на i-м шаге криптоанализа.

Подставив (14) в (13), получаем

$$C_1\left(\Phi_{CD_X},S\right)=\sum_i p(e_i)\times$$

$$\times\left[\int_{-\infty}^{\infty}P(k_{Bi}/e_i)\log\sqrt{2\pi\sigma_i^2}dk_{Bi}+\right.$$

$$\left.\int_{-\infty}^{\infty}P(k_{Bi}/e_i)\frac{k_{Bi}-e_i}{2\sigma_i^2}\log e dk_{Bi}\right].$$

Откуда с учетом того, что

$$\int P(k_{Bi}/e_i)(k_{Bi}-e_i)dk_{Bi}=\sigma_i^2$$

имеем

$$C_1\left(\Phi_{CD_X},S\right)=\sum_i P(e_i)\left[\log\sqrt{2\pi\sigma_i^2}+\frac{1}{2}\log e\right]=$$

$$=\frac{1}{2}\log(2\pi e\sigma^2).$$

Принимаем во внимание, что дисперсия условного распределения при криптоанализе σ^2 с позиций введенных выше допущений может быть представлена как $\sigma^2=\sigma_K^2-\sigma_E^2$, где σ_K^2 — дисперсия виртуального ключа, а σ_E^2 — дисперсия значений криптограмм. Тогда выражение (13) можно привести к виду

$$C_1\left(\Phi_{CD_X},S\right)=\frac{1}{2}\log(2\pi e\,[\sigma_K^2-\sigma_E^2]). \qquad (15)$$

Подставив (14) в (12), получим выражение эффективности виртуальной защиты для первого уровня криптоанализа виртуального скремблирования

$$D_1\left(\Phi_{CD_X},S\right)=\frac{1}{2}\log(2\pi e\,[\sigma_K^2-\sigma_E^2])-H[Y_p]. \quad (16)$$

Выражения (15) и (16) определяют нижнюю границу стойкости и эффективности защиты непрерывной информации при виртуальном скремблировании. Их анализ позволяет прийти к ряду практически важных выводов.

Во-первых, виртуальное скремблирование способно обеспечить значения стойкости и эффективности защиты непрерывной информации, соответствующие области теоретической недешифруемости. Причем для этого достаточно выполнить практически просто реализуемое условие:

$$\frac{1}{2}\log\left(2\pi e\left(\sigma_K^2-\sigma_E^2\right)\right)\geq H[Y_p].$$

Во-вторых, дисперсия виртуального ключа может иметь определяющее значение при решении задач повышения эффективности виртуального скремблирования. Так, приближение значений σ_K^2 к бесконечно большим величинам, $\sigma_K^2\to\infty$, вызывает соответствующее увеличение эффективности скремблирования $D_1\left(\Phi_{CD_X},S\right)\to\infty$. Это свидетельствует о потенциальной возможности выполнения условий абсолютной недешифруемости при виртуальном скремблировании путем соответствующего увеличения дисперсии ансамбля виртуальных ключей.

Необходимо подчеркнуть, что данные выводы относятся только к первому уровню защиты от криптоанализа, которую обеспечивает виртуальное скремблирование. При этом из них следует, что даже на этом уровне виртуальное скремблирование способно обеспечивать эффективность скремблирования, значительно превышающую эффективность известных подходов к защите непрерывной информации.

ВЫВОДЫ

1. Особенностью виртуализации процесса защиты непрерывной информации является возможность использования в качестве непрерывного ансамбля виртуализации исходного ансамбля источника сообщений.

2. При виртуализации ансамбля ключей путем включения в состав совместного ансамбля виртуализации исходного ансамбля сообщений абсолютная недешифруемость сохраняется при сокращении (сжатии) множества исходных ключей до одного ключа.

3. Включение в совместный ансамбль виртуализации в качестве непрерывного ансамбля исходного ансамбля сообщений не устанавливает ограничений на объём выборочного пространства ансамбля ключевых данных.

4. Виртуализация процесса защиты непрерывной информации обеспечивает трехуровневую защиту с позиций криптоанализа ключа в отличие от одноуровневой, присущей для известных подходов.

5. Виртуальное скремблирование способно обеспечить значения стойкости и эффективности защиты непрерывной информации, соответствующие области теоретической недешифруемости.

Литература

[1] *Котенко В.В.* Теория виртуализации и защита телекоммуникаций: – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 244 с.

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

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

[4] *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.

[5] *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.

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

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

[8] *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 12.03.2013

Котенко Владимир Владимирович, фото и сведения об авторе см. на стр. 271.

Котенко Станислав Владимирович, фото и сведения об авторе см. на стр. 271.

Румянцев Константин Евгеньевич, фото и сведения об авторе см. на стр. 272.

Горбенко Юрий Иванович, фото и сведения об авторе см. на стр. 193.

УДК 621.3.06

Стратегія захисту безперервної інформації з позицій віртуалізації ансамблю ключів на формальні відносини ансамблів / В.В. Котенко, С.В. Котенко, К.Є. Румянцев, Ю.І. Горбенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 308–312.

Наводиться фундаментальне обґрунтування стратегії захисту безперервної інформації з позицій віртуалізації ансамблю ключів на формальні відносини ансамблів. Встановлюється, що застосування стратегії вперше відкриває можливість трирівневого захисту безперервної інформації. Оцінка ефективності захисту від криптоаналізу на першому (початковому) рівні захисту показує потенційну можливість виконання умов абсолютної недешифрувальності шляхом відповідного збільшення дисперсії ансамблю віртуальних ключів.

Ключові слова: ансамбль ключів, віртуалізація процесу захисту безперервної інформації, обсяг вибіркового простору ансамблю ключових даних, трирівневий захист безперервної інформації, ентропія віртуального ансамблю ключів.

Іл.: 2. Бібліогр.: 8 найм.

UDC 621.3.06

Continuous data protection strategy from the standpoint of virtualization of ensemble of keys on a formal relationship of ensembles / V.V. Kotenko, S.V. Kotenko, K.E. Rumyantsev, Yu.I. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 308–312.

Fundamental justification of continuous information protection strategy from the positions of virtualization of an ensemble of keys on of ensembles is given. It is found that the strategy application opens for the first time a formal relations possibility of three-level protection of continuous information. The assessment of efficiency of protection against cryptanalysis at the first (initial) level of protection shows a potential possibility of satisfying the conditions of an absolute indecipherability by the corresponding increase of dispersion of an ensemble of virtual keys.

Keywords: : ensemble of key data, virtualization of continuous information protection process, amount of sample space of key data ensemble, three-level protection of continuous information, entropy of a virtual key ensemble.

Fig.: 2. Ref.: 8 items.