2. *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.
3. *Котенко С.В., Румянцев К.Е.* Компьютерное моделирование технологии аурикулодиагностической идентификации // Тр. науч.-техн. конф. с международным участием «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2010). Ч. 2. – Харьков: Изд-во ХНУ, 2010. – С. 128-131.
4. *Румянцев К.Е., Котенко С.В.* Эффективность виртуальной аурикулодиагностической идентификации // Материалы XI Международной науч.-практ. конф. «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 170-175.
5. *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 // Proceeding of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery. – New York. 2009. – P. 235-239.
6. *Румянцев К.Е., Котенко С.В.* Идентификация личности на основе формирования оценки виртуального персонального образа // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 73-75.
7. *Румянцев К.Е., Котенко С.В.* Идентификация личности на основе формирования оценки виртуального персонального образа // Информационное противодействие угрозам терроризма. – 2006. – № 8. – С. 73-75.
8. *Котенко С.В.* Комплекс аурикулодиагностической идентификации // Информационное противодействие угрозам терроризма. – 2011. – № 16. – С. 73-79.

Статью рекомендовал к опубликованию д.т.н., профессор Г.А. Галуев.

Котенко Станислав Владимирович – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: stassecurity@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634315507; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Kotenko Stanislav Vladimirovich – Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: stassecurity@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: 88634315507; the department of information security of telecommunication systems; postgraduate student.

УДК 621.39

В.В. Котенко

ЗАЩИТА ДИСКРЕТНОЙ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ

Приводится фундаментальное решение задачи оптимизации процесса защиты дискретной информации с позиций виртуализации информационных потоков.На основе теоретического обоснования условий виртуализации осуществляется синтез алгоритмов и моделей шифрования (дешифрования), обеспечивающего оптимизацию информационного потока. Виртуализация реализуется включением на выходе преобразования шифрования и на входе преобразования дешифрования модуля виртуализации информационного потока, осуществляющего дешифрования криптограмм исходного и виртуального информационных потоков, шифрование результатов дешифрования и задержки во времени ключевых последовательностей и сообщений.

Защита информации; шифрование; виртуализация; оптимизация; информационный поток.

V.V. Kotenko

PROTECTION OF THE DISCRETE INFORMATION FROM POSITIONS VIRTUALIZATIONS OF INFORMATIVE STREAMS

The fundamental decision of a problem of optimization of process of protection of the discrete information from positions virtualizations of informative streams.On the basis of theoretical explanation of virtualization is synthesis algorithms and encryption (decryption) models for optimization of information flow. Virtualization is the inclusion in the transformation output encryption and decryption in the transformation input module virtualization information flow, performing decryption cryptograms source and virtual information flows, encryption and decryption results delay time message and key sequences.

Information protection; enciphering, virtualizations; optimization; an informational stream.

Защиту информации дискретного источника можно представить в виде преобразования информационного потока, изначально представляющего поток сообщений. Форма этого потока в ходе шифрования подвергается изменениям. Эти изменения вызываются предусмотренными преобразованиями защиты дискретной информации. В общем виде форма информационного потока на выходе источника информации характеризуется средним количеством информации $I[U]$ ансамбля сообщений источника. В ходе преобразования защиты дискретной информации (шифрования) Φ ансамбль источника преобразуется к форме ансамбля криптограмм E. Таким образом, процесс изменения формы информационного потока характеризуется выражением

$$I[U;E] = I[U] - I[U/E], \tag{1}$$

где $I[U/E]$ характеризует преобразование Φ, описываемое как инъективное отображение элементов ансамбля U в элементы ансамбля E, заданное ансамблем ключа K:

$$\Phi : U \xrightarrow[\uparrow K]{} E \quad . \tag{2}$$

Преобразование (2) считается прямым преобразованием. Тогда преобразование элементов ансамбля криптограмм в элементы ансамбля сообщений определяется, как обратное преобразование Φ^{-1}. Учитывая свойство симметричности средней взаимной информации в (1), обратное преобразование Φ^{-1} однозначно характеризуется средней условной информацией $I[E/U]$.

Пусть ставится задача оптимизации изменения формы информационного потока при шифровании относительно известного условия

$$I\left[U^*;E^*\right] = 0. \tag{3}$$

С позиций теории виртуализации условие (3) определяет *условие виртуализации 1*.

Условие 1. Изменение формы информационного потока при шифровании оптимально, если $I\left[U^*;E^*\right] = 0$.

Тогда виртуализация, определяемая условием (3) с учетом (2), состоит в инъективном отображении совместного ансамбля UEK в совместный ансамбль $U^*E^*K^*$:

$$vir(I[U;E]) : UEK \to U^*E^*K^*, \tag{4}$$

где общий вид процесса виртуализации характеризуется как

$$I[U;E] + \Psi\left[I;I^*\right] = I\left[U^*;E^*\right]. \tag{5}$$

Из (5) следует, что выполнение условия (3) требует изменения характеристики преобразования формы информационного потока (1) на величину $\Psi\left[\mathrm{I};\mathrm{I}^{*}\right]$, определяемую как *функционал виртуализации*.

Теорема 1. Пусть $\mathrm{I}[\mathrm{U};\mathrm{E}]$ – характеристика изменения формы информационного потока при шифровании. Тогда если условие виртуализации $\mathrm{I}[\mathrm{U}^{*};\mathrm{E}^{*}]=0$, то функционал виртуализации, обеспечивающий оптимизацию информационного потока относительно данного условия, определяется как

$$\Psi\left[\mathrm{I};\mathrm{I}^{*}\right]=\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]. \tag{6}$$

Доказательство. С учетом условия (4) выражение (5) приводится к виду

$$\Psi\left[\mathrm{I};\mathrm{I}^{*}\right]=-\mathrm{I}\left[\mathrm{U};\mathrm{E}\right]. \tag{7}$$

Согласно [1], имеем

$$\mathrm{I}\left[\mathrm{U};\mathrm{E}\right]=\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]. \tag{8}$$

Подставив (8) в (7), окончательно получаем

$$\Psi\left[\mathrm{I};\mathrm{I}^{*}\right]=\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right].$$

что и требовалось доказать.

Функционал виртуализации в (5) формирует проекцию на область абсолютно оптимальных решений, заданную условием виртуализации 1.

Учитывая, что ансамбль U является ансамблем источника, задача оптимизации информационного потока сводится к оптимизации формы представления информационного потока на выходе преобразования шифрования $\mathrm{I}[\mathrm{E}]$, т.е. к определению $\mathrm{I}[\mathrm{E}^{*}]$. Подставив в (5) выражение для функционала виртуализации (6) и преобразовав $\mathrm{I}[\mathrm{U}^{*};\mathrm{E}^{*}]$ на основании свойства симметричности взаимной информации, получим

$$\mathrm{I}\left[\mathrm{E}\right]-\mathrm{I}\left[\mathrm{E}/\mathrm{U}\right]+\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]=\mathrm{I}\left[\mathrm{E}^{*}\right]-\mathrm{I}\left[\mathrm{E}^{*}/\mathrm{U}^{*}\right], \tag{9}$$

откуда

$$\mathrm{I}\left[\mathrm{E}^{*}\right]=\mathrm{I}\left[\mathrm{E}\right]+\left(\mathrm{I}\left[\mathrm{E}^{*}/\mathrm{U}^{*}\right]-\mathrm{I}\left[\mathrm{E}/\mathrm{U}\right]\right)+\left(\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]\right). \tag{10}$$

Определим выражение для $\left(\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]\right)$:

$$\begin{aligned}\mathrm{I}\left[\mathrm{K}/\mathrm{U}\right]\text{-}\mathrm{I}\left[\mathrm{K}/\mathrm{UE}\right]&=\mathrm{I}\left[\mathrm{K}\right]+\mathrm{I}\left[\mathrm{U}/\mathrm{K}\right]-\mathrm{I}\left[\mathrm{U}\right]-\mathrm{I}\left[\mathrm{K}\right]-\mathrm{I}\left[\mathrm{UE}/\mathrm{K}\right]+\mathrm{I}\left[\mathrm{E}\right]+\mathrm{I}\left[\mathrm{U}/\mathrm{K}\right]=\\&=\mathrm{I}\left[\mathrm{E}\right]+\mathrm{I}\left[\mathrm{U}/\mathrm{E}\right]-\mathrm{I}\left[\mathrm{U}\right]+\left(\mathrm{I}\left[\mathrm{U}/\mathrm{K}\right]-\mathrm{I}\left[\mathrm{UE}/\mathrm{K}\right]\right)=\\&=\mathrm{I}[\mathrm{U}/\mathrm{E}]+\mathrm{I}[\mathrm{U}/\mathrm{E}]+\mathrm{I}[\mathrm{K}]-\mathrm{I}[\mathrm{U}]+\mathrm{I}[\mathrm{U}/\mathrm{K}]-\mathrm{I}[\mathrm{U}/\mathrm{KE}].\end{aligned} \tag{11}$$

Подставив (11) в (10), окончательно получим:

$$\mathrm{I}[\mathrm{E}^{*}]=\mathrm{I}[\mathrm{E}]+\left((\mathrm{I}[\mathrm{E}^{*}/\mathrm{U}^{*}]-\mathrm{I}[\mathrm{E}/\mathrm{U}])+(\mathrm{I}[\mathrm{K}]-\mathrm{I}[\mathrm{U}])\right)+(\mathrm{I}[\mathrm{U}/\mathrm{E}]+\mathrm{I}[\mathrm{K}/\mathrm{E}]). \tag{12}$$

Выражение (12) отражает общий вид решения задачи оптимизации формы преобразования информационного потока при шифровании относительно условия виртуализации 1. С этих позиций $\mathrm{I}[\mathrm{E}^{*}]$ можно рассматривать как проекцию формы представления информационного потока на выходе преобразования шифрования на область абсолютно оптимальных решений, заданную условием виртуализации 1. Переход от общего решения (12) к конкретным решениям обеспечивается введением следующих условий виртуализации.

Условие 2. Средняя условная взаимная информация I[U/E] характеризует прямое преобразование шифрования Ф элементов ансамбля U в элементы ансамбля E.

Условие 3. Средняя условная взаимная информация I[E/U] однозначно характеризует обратное преобразование однозначно Φ^{-1} элементов ансамбля E в элементы ансамбля U.

Условие 4. Сумма условных взаимных информаций I[E/U]+(I[U/E]+I[K/E]) характеризует прямое преобразование шифрования Ф от обратного преобразования шифрования Φ^{-1}.

Условия виртуализации 2–4 открывают возможность проекции общего решения (12) на выборочное пространство совместного ансамбля $XYKX^*Y^*K^*$. Осуществив привязку этой проекции ко времени, окончательно получаем

$$e_i^* = e_i + \Phi_{k_{i-l}}\left(\Phi^{-1}_{k_{i-r}}(e^*_{i-r}) - \Phi^{-1}_{k_{i-n}}(e_{i-n}) + (k_{i-j} - u_{i-p})\right). \qquad (13)$$

Выражение (13) представляет алгоритм шифрования, обеспечивающий оптимизацию информационного потока относительно условия виртуализации $I[U^*;E^*]=0$. Модель шифрования, соответствующая этому алгоритму, приведена на рис. 1.

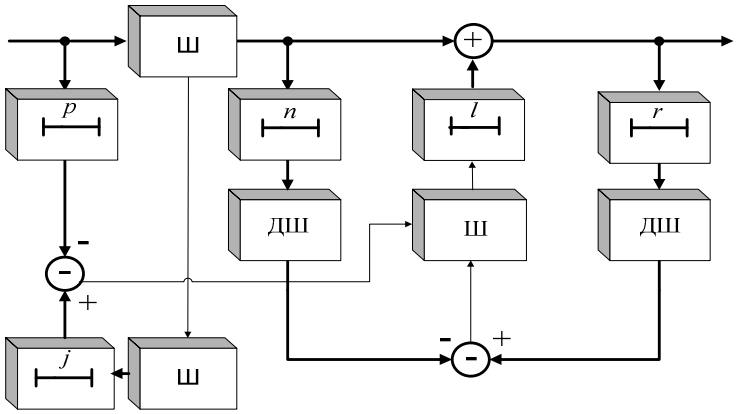

Рис. 1. Модель шифрования, обеспечивающего оптимизацию информационного потока относительно условия виртуализации $I[U^*;E^*]=0$

Девиртуализация, определяемая условием (3), состоит в инъективном отображении совместного ансамбля $U^*E^*K^*$ в совместный ансамбль UEK:

$$dvir(I[U;E]): U^*E^*K^* \rightarrow UEK, \qquad (14)$$

где общий вид процесса виртуализации характеризуется как

$$I[U;E]=I\left[U^*;E^*\right] - \Psi\left[I;I^*\right]. \qquad (15)$$

Функционал виртуализации в (15) формирует проекцию области абсолютно оптимальных решений, заданной условием виртуализации 1, на область решений, определенную постановкой задачи. Подставив в (15) выражение для функционала виртуализации (6), получим общий вид решения задачи девиртуализации оптимальной формы представления информационного потока на входе преобразования дешифрования относительно условия виртуализации 1, определяемого выражением (3):

$$I[E^*]=I[E]+\left((I[E^*/U^*]-I[E/U])+(I[K]-I[U])\right)+(I[U/E]+I[K/E]). \quad (16)$$

Применив к (16) условия виртуализации 2–4 и осуществив привязку ко времени, получаем

$$e_i = e_i^* - \Phi_{k_{i-l}}\left(\Phi^{-1}_{k_{i-r}}(e^*_{i-r}) - \Phi^{-1}_{k_{i-n}}(e_{i-n}) + (k_{i-j} - u_{i-p})\right). \quad (17)$$

Принимая во внимание, что $x_i = \Phi_i^{-1}(y_i)$, окончательно имеем:

$$u_i = \Phi^{-1}_{k_i}\left(e_i^* - \Phi_{k_{i-l}}\left(\Phi^{-1}_{k_{i-r}}(e^*_{i-r}) - \Phi^{-1}_{k_{i-n}}(e_{i-n}) + (k_{i-j} - u_{i-p})\right)\right). \quad (18)$$

Выражение (18) представляет алгоритм дешифрования, обеспечивающий оптимизацию информационного потока относительно условия $I[U^*;E^*]=0$. Модель дешифрования, соответствующая этому алгоритму, приведена на рис. 2.

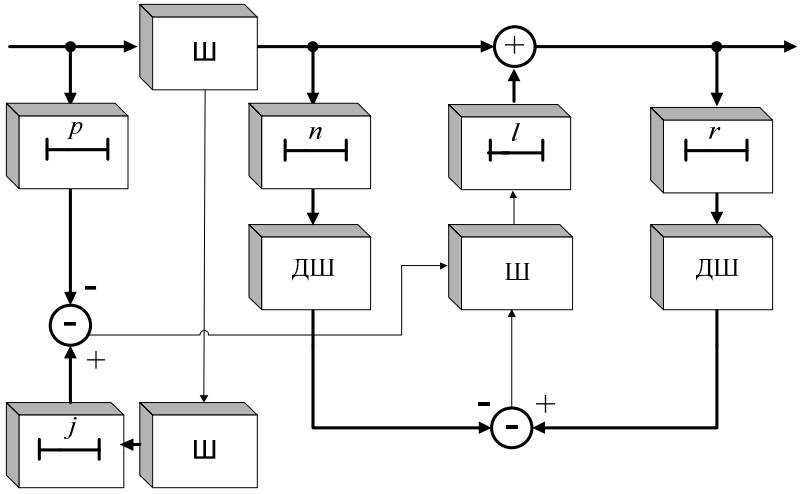

Рис. 2. Модель дешифрования, обеспечивающего оптимизацию информационного потока относительно условия виртуализации $I[U^*;E^*]=0$

Анализ моделей рис. 1–2 показывает, что виртуализация реализуется включением на выходе преобразования шифрования и на входе преобразования дешифрования модуля виртуализации информационного потока (МВП), осуществляющего дешифрования криптограмм исходного и виртуального информационных потоков, шифрование результатов дешифрования и задержки во времени ключевых последовательностей и сообщений. Это обеспечивает оптимизацию исходных преобразований шифрования и дешифрования, характеризуемую следующими дополнительно открывающимися возможностями. Во-первых, включение дополнительного преобразования шифрования обеспечивает возможность повышения стойкости защиты информации. Применительно к цифровой идеологии современных телекоммуникаций, позволяющей реализовывать операции сложения и вычитания посредством операции сложения по модулю 2, повышение стойкости защиты в данном случае может достигаться при неизменной исходной длине криптограмм. Образно говоря, осуществляется шифрование в шифровании, при этом сдвиг криптограмм повторного шифрования во времени можно трактовать как их повторную передачу. Во-вторых, появляется возможность идентификации и аутентификации источника информации. В качестве идентификатора источника при этом выступает последовательность значений

задержек $lrnpj$, устанавливаемых в модуле временных задержек. В-третьих, сложение исходных криптограмм с криптограммами повторного шифрования можно интерпретировать как преобразование защиты информации. При этом включение исходных и виртуальных сообщений в формирование ключевой последовательности будет обеспечивать решение задачи имитозащиты.

Программная реализация моделей рис. 1–2 применительно к известным шифрам DES и AES (рис. 3) показала, что применение модулей виртуализации информационного потока обеспечивает значительное увеличение эффективности шифрования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Котенко В.В., Румянцев К.Е.* Теория информации и защита телекоммуникаций: Монография. – Ростов-на-Дону: Изд-во ЮФУ, 2009. – 369 с.
2. *Котенко В.В.* Теоретическое обоснование виртуальных оценок в защищенных телекоммуникациях // Материалы XI Международной науч.-практ. конф. «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 177-183.
3. *Котенко В.В.* Теоретические основы виртуализации представления объектов, явлений и процессов // Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 32-48.
4. *Котенко В.В.* Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 69-80.
5. *Котенко В.В.* Виртуализация процесса защиты дискретной информации относительно условий теоретической недешифруемости // Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 80-96.
6. *Котенко В.В.* Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа // Информационное противодействие угрозам терроризма. – 2011. – № 17. – С. 96-104.
7. *Котенко В.В.* Новый подход к оценке информационного образа объекта исследования с позиций теории виртуального познания // Информационное противодействие угрозам терроризма. – 2005. – № 4. – С. 34-41.

Статью рекомендовал к опубликованию д.т.н., профессор Г.А. Галуев.

Котенко Владимир Владимирович – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: virtsecurity@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634315507; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; доцент.

Kotenko Vladimir Vladimirovich – Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: virtsecurity@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634315507; the department of information security of telecommunication systems; cand. of eng. sc.; associate professor.