БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Помазанов А.В., Хоменко Д.А.* Способ повышения пропускной способности комплекса радиоконтроля // Известия ТРТУ. – 2003. – № 4 (33). – С. 328-329.
2. *Помазанов А.В.* Оценка девиации частоты ЧМ-сигналов с немонотонными законами изменения частоты // Тезисы докл. 3 ВНТК «Методы и средства измерений физических величин». Ч. 10. – Н. Новгород: НГТУ, 1998. – С. 33.
3. *Роздобудько В.В., Помазанов А.В. и др.* Акустооптический измеритель частотно-временных параметров СВЧ-радиосигналов // Специальная техника. – 2011. – № 3. – С.8-24.

Статью рекомендовал к опубликованию д.т.н., профессор В.И. Марчук.

Помазанов Александр Васильевич – Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге; e-mail: pav_tsure@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371902; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; доцент.

Pomazanov Alexandr Vasil'evich – Taganrog Institute of Technology **–** Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: pav_tsure@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; тел.: +78634371902; the department of information security of telecommunication systems; head the department; cand. of eng. sc.; associate professor.

УДК 621.39

С.В. Котенко

СТРАТЕГИЯ МНОГОФАКТОРНОЙ ИДЕНТИФИКАЦИИ С ПОЗИЦИЙ СИНТЕЗА ВИРТУАЛЬНЫХ ОБРАЗОВ ИДЕНТИФИКАТОРОВ

Впервые предложена стратегия решения задачи многофакторной идентификации с позиций синтеза виртуальных образов идентификаторов. Определяется теоретически обоснованный комплекс условий виртуализации, относительно которого синтезируется алгоритм формирования виртуальных образов на основе унификации информационных оценок идентификаторов. При этом не накладывается ограничений на выбор процедуры унификации, что открывает качественно новый уровень возможностей многофакторной идентификации,эффективность которых подкрепляется приведенными результатами экспериментальных исследований.Экспериментальная проверка проводилась путем тестирования макета системы многофакторной персональной аутентификации,реализованного на основе синтезированного алгоритма.

Идентификация; аутентификация; виртуализация; виртуальный образ; информационный поток.

S.V. Kotenko

STRATEGY OF MULTIVARIABLE AUTHENTICATION FROM POSITIONS OF SYNTHESIS OF VIRTUAL CHARACTERS OF IDENTIFIERS

For the first time proposed a strategy to address the challenges of multi-factor identification from the perspective of virtual images. Defines a theoretically well-founded set conditions of virtualization, which is synthesized algorithm generate virtual images on the basis of the unification of information evaluation identifiers. There is restriction on the choice of procedure harmonization, which opens up a new level of multifactor authentication, which is supported by the results of the pilot studies. Pilot testing was carried out by testing the layout system of multi-factor authentication available on a personalized basis of synthesized algorithm.

Identification; authentification; virtualization; the virtual image; an informational stream.

С позиций информационного анализа идентификация представляется в виде схемы коммуникации [1], где объект идентификации выступает в роли источника информации. Реальные объекты при их включении в схему коммуникации представляют собой непрерывные источники информации. Главной особенностью рассматриваемой коммуникации является то, что восприятие количества информации об идентификаторах объекта получателем осуществляется квантами $\mathbf{J}(t) = \mathbf{J}(i)$. Эта ситуация является типичной для современных подходов к обработке информации об объектах идентификации. С этих позиций задача идентификации состоит в оценке компонент вектора $\mathbf{J}(i)$. Решение этой задачи в прямой постановке возможно на основе подходов теории виртуализации [2].

Основываясь на проведенных рассуждениях, определим условия виртуализации.

Условие 1. Количество собственной информации идентификаторов объекта является вещественной величиной.

Условие 2. Количество собственной информации идентификаторов объекта во времени представляет векторный непрерывный случайный процесс.

Условие 3. Восприятие информации об идентификаторах объекта осуществляется квантами.

Условие 4. Основной задачей получателя информации в ходе идентификации объекта является формирование информационного образа источника информации.

Установленный комплекс условий определяет область возможных решений оптимальной идентификации объекта. Изменение представления объекта в этих условиях определяется как виртуализация. При этом множественность установленных условий определяет возможную множественность этапов виртуализации. Однако в конечном итоге решение задачи сводится к инъективному отображению ансамбля наблюдений J в ансамбль оценок $\tilde{\mathbf{J}}^*$:

$$vir(\mathbf{J}(t)) : \mathrm{J} \rightarrow \tilde{\mathbf{J}}^* . \qquad (1)$$

Реализация (1) состоит в решении задачи определения оценки $\tilde{\mathbf{J}}^*(t)$ исходного процесса $\tilde{\mathbf{J}}(t)$ по наблюдению $\mathbf{J}(t)$, обеспечивающей минимально допустимую величину ошибки $\mathbf{e}(t) = \tilde{\mathbf{J}}(t) - \tilde{\mathbf{J}}^*(t)$.

С позиций обоснованных в [2] фундаментальных производных предложений поставленную задачу можно рассматривать как реальную проекцию некоторого виртуального образа, позволяющую получателю свести к минимуму потери информации идентификаторов источника. Среди возможных реальных проекций наибольший интерес в нашем случае представляет задача минимизации ошибки оценивания дискретных сообщений. Виртуальная аналогизация относительно этой задачи позволяет получать достаточно оригинальный подход к решению задачи, определяемой (1):

$$\mathbf{J}^*(i+1) = \mathbf{J}^*(i+1/i) + \mathbf{K}(i+1)(\mathbf{J}_\psi(i+1) - \mathbf{H}(i+1)\mathbf{J}^*(i+1/i)), \qquad (2)$$

где $\mathbf{J}^*(i+1)$ – оценка вектора состояния на момент времени (*i+1*); $\mathbf{J}^*(i+1/i)$ – вектор предсказанных оценок на момент времени (*i+1*) по данным на шаге *i*; $\mathbf{J}_\psi(i+1)$ – вектор наблюдений; $\mathbf{H}(i+1)$ - матрица наблюдений; $\mathbf{K}(i+1)$ – матрица весовых коэффициентов; $\mathbf{J}^*(i+1/i) = \mathbf{\Phi}(\mathbf{J}^*, i)$ – матричное уравнение для расчета вектора предсказания.

Матрица весовых коэффициентов определяется как

$$\mathbf{K}(i+1) = \mathbf{P}(i+1/i)\mathbf{H}^T(i+1)\left[\mathbf{H}(i+1)\mathbf{P}(i+1/i)\mathbf{H}^T(i+1) + \mathbf{R}_E(i+1)\right], \qquad (3)$$

где $\mathbf{P}(i+1/i)=\mathbf{F}\mathbf{P}(i/i)\mathbf{F}^T$ – апостериорная матрица ковариаций ошибок предсказания; $\mathbf{F}(\mathbf{J}^*,i)=\partial\mathbf{\Phi}(\mathbf{J}^*,i)/\partial\mathbf{J}^*$ – матрица Якоби от $\mathbf{\Phi}(\mathbf{J}^*,i)$; $\mathbf{R}_E(i+1)$ – диагональная ковариационная матрица шумов наблюдения.

В выражении (3) априорная матрица ковариации ошибок оценивания $\mathbf{P}(i/i)$ представляется в виде

$$\mathbf{P}(i/i)=\left[\mathbf{I}-\mathbf{K}(i)\mathbf{H}\right]\mathbf{P}(i/i-1),$$

где $\mathbf{I}$ – диагональная единичная матрица.

Для инициации работы алгоритма (1)–(3)необходимо задать начальные значения матрицы ковариации ошибок оценивания $\mathbf{P}(0/0)$, начальный вектор оценок $\mathbf{J}^*(0)$ и диагональные элементы корреляционной матрицы ошибок наблюдения $\mathbf{R}_E(i+1)$. Начальные значения вектора $\mathbf{J}^*(0)$ могут быть заданы как средние величины, исходя из предполагаемых значений средних количеств информации в идентификаторах. Априорная корреляционная матрица ошибок оценивания является диагональной, значения элементов которой соответствуют дисперсиям ошибок идентификации в начальный момент времени.

Согласно условиию 4 ансамбль U оценок $\mathbf{J}^*(i)$ используется для формирования информационного образа, которое состоит в инъективном отображении ансамбля U в ансамбль G:

$$vir(\mathbf{J}^*(i)):\mathrm{U}\rightarrow\mathrm{G}. \tag{4}$$

Элементы выборочного пространства ансамбля G являются векторными величинами с числом компонент, равным числу информационных каналов виртуализации:

$$\mathbf{G}_\mathrm{J}=\left\|\mathrm{G}_{\mathrm{J}n}\right\|=\left\|2(S^*_{\mathrm{J}n})^2\right\|, \tag{5}$$

где $S^*_{\mathrm{J}n}$ – информационный образ относительно n-го канала виртуализации;

$$S^*_{\mathrm{J}n}=\int_0^\infty \mathrm{J}^*_n(t)\exp\left(-j\omega t\right)dt. \tag{6}$$

Формирование информационного образа объекта осуществляется путем унификации компонент вектора $\mathbf{G}_\mathrm{J}$:

$$\Re=unif\left(\mathrm{G}_{\mathrm{J}n}\right). \tag{7}$$

Информационный образ (7) получен при установленных условиях виртуализации 1–4, что дает основание его определения как *виртуальный информационный образ,* или сокращенно – *виртуальный образ*. Суть процедуры унификации состоит в формировании на основании $\mathrm{G}_{\mathrm{J}n}$ пространственного образа в n-мерном пространстве. При этом не накладывается ограничений на выбор процедуры унификации, что открывает качественно новый уровень возможностей для представления объектов, явлений и процессов. Как показали исследования, реализация этих возможностей приводит к принципиально новым решениям задач идентификации и аутентификации.

Основу реализации стратегии идентификации (1)–(7) составляют блок-схемы алгоритмов идентификации на основе комплексной многофакторной информационной виртуализации идентификаторов. Совокупность этих алгоритмов определяет дискретную модель системы многофакторной аутентификации. Экспериментальная проверка проводилась путем тестирования реализованного макета систе-

мы многофакторной персональной аутентификации. В ходе тестирования на основе персональных биометрических идентификаторов строились информационные и виртуальные образы. На основе полученного видеоизображения система формирует два информационных образа. Таким образом, виртуальный образ строится на основе двух информационных образов, полученных из одного персонального идентификатора путем горизонтальной и вертикальной развертки видеоизображения. Уровень идентичности определяется путем взаимного корреляционного анализа двух трехмерных виртуальных образов: эталонного и текущего.

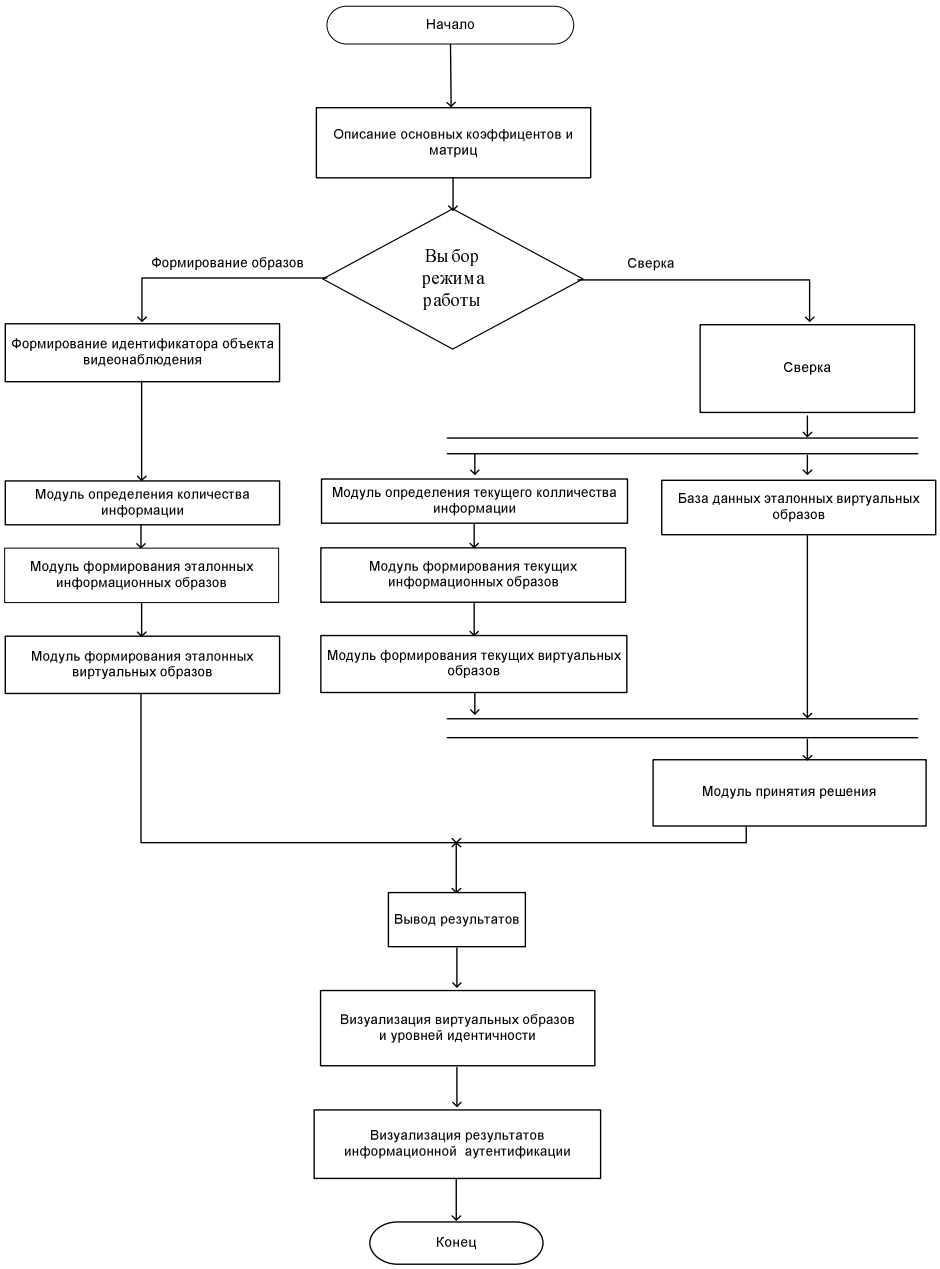

Рис. 1. Дискретная модель системы многофакторной аутентификации

Для оценки эффективности системы исследовались следующие топологии идентификации: 1) однофакторная идентификация; 2) многофокторная идентификация; 3) однофакторная аутентификация; 4.Многофакторная аутентификация.

Диаграмма значений точности идентификации относительно диапазонов уровней идентичности, полученных на основе многофакторной идентификации персональных идентификаторов, приведена на рис. 2. Зависимость погрешности многофакторной идентификации персональных идентификаторов от граничных уровней идентичности отражена на рис. 3.

С позиций исследуемого подхода открывается возможность количественной оценки эффективности аутентификации (определения истинности идентификатора). Принимая во внимание, что в качестве анализируемого идентификатора в данном случае выступает ложный идентификатор, повышение эффективности аутентификации характеризуется уменьшением значения уровня идентичности.

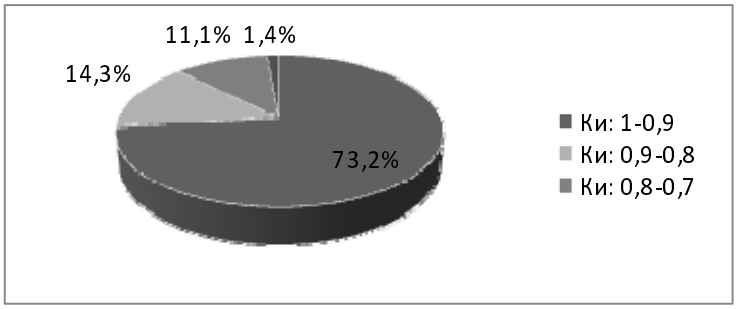

Рис. 2. Диаграмма значений точности идентификации при многофакторной идентификации персональных идентификаторов

Рис. 3. Зависимость погрешности многофакторной идентификации персональных идентификаторов от граничных уровней идентичности

Результаты исследования уровня идентичности виртуальных информационных образов истинного базового (индивидуум 1) и ложного анализируемого (индивидуум 2) идентификаторов показывают, что при граничном значении уровня идентичности $К_И = 6$ погрешность аутентификации равна нулю. Таким образом, обеспечивается абсолютная точность аутентификации. Это свидетельствует о принципиально новом классе эффективности аутентификации.

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 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.