ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

4

(131)

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2020

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

4 (131)

Москва 2020
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2020.
Вып. 4 (131). С. 1—52.

Редактор *О. А. Константинова*
Компьютерная верстка: *Н. В. Ильина*, *К. В. Трыкина*

Подписано в печать 10.12.2020. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 6,0. Уч.-изд. л. 6,2.
Тираж 400 экз. Заказ 1963. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано в ООО "РАПИТОГРАФ".
117342, Москва, ул. Бутлерова, д. 17Б.
Индекс 79187.

ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 003.26

Постквантовая схема открытого распределения ключей

Д. Н. Молдовян, канд. техн. наук; *А. А. Молдовян,* д-р техн. наук
ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, Россия

Предложен новый способ построения протоколов открытого распределения ключей, основанных на скрытой задаче дискретного логарифмирования, заданной в конечной некоммутативной ассоциативной алгебре с глобальной двухсторонней единицей. Способ отличается использованием двух взаимно коммутативных операций, маскирующих базовую операцию экспоненцирования в циклической группе простого порядка, имеющего достаточно большую разрядность. Описана реализующая способ криптосхема, алгебраическим носителем которой является четырехмерная алгебра с множеством локальных левосторонних единиц, задаваемым в аналитическом виде. Разработанная криптосхема представляет интерес для построения постквантовых протоколов открытого распределения ключей.

Ключевые слова: защита информации, криптография, открытое согласование ключей, задача дискретного логарифмирования, конечная ассоциативная алгебра, некоммутативная алгебра, глобальная единица, локальная единица, левосторонняя единица.

В текущее время актуальна проблема разработки практичных постквантовых алгоритмов и протоколов с открытым ключом [1—3], что связано с прогнозами появления в близком будущем многокубитового квантового компьютера. Двухключевые криптосхемы, основанные на вычислительной сложности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), в постквантовую эру становятся небезопасными в силу известных полиномиальных алгоритмов решения ЗДЛ и ЗФ на квантовом компьютере [4—6]. Полиномиальные алгоритмы решения этих двух вычислительных задач строят по схеме сведения к задаче нахождения длины периода периодической функции, задаваемой по известным параметрам криптосхемы. В случае решения ЗДЛ на квантовом компьютере строят периодическую функцию, принимающую значения в явно заданной циклической группе и содержащую период, длина которого зависит от значения логарифма.

Молдовян Дмитрий Николаевич, научный сотрудник лаборатории "Кибербезопасность и постквантовые криптосистемы".
E-mail: mdn.spectr@mail.ru
Молдовян Александр Андреевич, профессор, главный научный сотрудник лаборатории "Кибербезопасность и постквантовые криптосистемы".
E-mail: maa1305@yandex.ru

Статья поступила в редакцию 19 января 2020 г.

Разработка постквантовых криптосхем с открытым ключом связана с использованием в качестве базового криптографического примитива вычислительно-сложных задач, отличающихся от ЗДЛ и ЗФ [7]. Сравнительно новым подходом является построение схем ЭЦП, основанных на вычислительной трудности задачи дискретного логарифмирования в скрытой циклической группе [8], называемой также скрытой задачей дискретного логарифмирования (СЗДЛ). Алгебраическими носителями СЗДЛ и двухключевых криптосхем на ее основе являются конечные некоммутативные группы и конечные некоммутативные ассоциативные алгебры (КНАА) [9, 10].

Обоснование СЗДЛ как базового примитива криптосхем с открытым ключом заключается в том, что общие параметры криптосхемы и открытый ключ представляют собой элементы КНАА, принадлежащие двум или более различным конечным группам, являющимся подмножествами элементов КНАА, используемой в качестве алгебраического носителя криптосхемы. Поэтому задание периодических функций по известным параметрам криптосхемы, содержащих период, зависящий от значения вычисляемого логарифма, приводит к случаям формирования функций, принимающих значения элементов КНАА, относящихся к достаточно большому числу различных конечных групп. При этом известные квантовые алго-

ритмы решения ЗДЛ используют возможность квантового вычислителя чрезвычайно эффективно выполнять дискретное преобразование Фурье [11, 12] и находить длины периодов для случая периодических функций, принимающих значения в рамках одной конечной группы.

Ранее для построения постквантовых протоколов открытого распределения ключей рассматривали криптосхемы, основанные на задании СЗДЛ в конечной алгебре кватернионов и использовании операции автоморфного отображения в качестве процедуры, маскирующей базовую операцию экспоненцирования. Однако в работах [13—15] были предложены способы сведения СЗДЛ в конечной алгебре кватернионов к обычной ЗДЛ в конечном поле.

В данной работе рассмотрен способ построения протокола открытого распределения ключей, основанный на СЗДЛ, при использовании двух различных маскирующих операций. Описана новая четырехмерная КНАА, используемая в качестве алгебраического носителя новой формы СЗДЛ. В предложенном способе и разработанной на его основе криптосхеме использованы наличие в алгебре большого множества локальных единиц и возможность их описания в виде метематической формулы.

Задача дискретного логарифмирования и механизмы маскирования

Для разработки протоколов открытого согласования ключей и электронной цифровой подписи (ЭЦП) обычно применяют ЗДЛ, задаваемую в конечной циклической группе. Традиционная формулировка ЗДЛ состоит в следующем: известен открытый ключ Y в виде элемента циклической группы, вычисленный по формуле

$$Y' = G^x,$$

где G — генератор группы простого порядка q, имеющего большую разрядность (от 256 до 4096 бит);

x — личный секретный ключ ($x < q$).

Вычисление значения x по заданным элементам G и Y' называется ЗДЛ. Для классического компьютера неизвестны алгоритмы с полиномиальной временной сложностью решения ЗДЛ в подгруппах мультипликативной группы простого конечного поля $GF(p)$ и в других конечных циклических группах.

Известный способ решения ЗДЛ на квантовом вычислителе включает задание периодической функции $f(i, j) = Y'^i G^j$ двух целочисленных переменных, i и j, которая имеет периоды следующих длин: $(0, q)$, $(q, 0)$, (q, q) и $(-1, x)$. Последнее значение связано с дискретным логарифмом:

$$Y'^i G^j = Y'^{i-1} G^{j+x} \Rightarrow f(i, j) = f(i-1, j+x).$$

Функция $f(i, j)$ принимает значения в заданной циклической группе. На квантовом компьютере за полиномиальное время можно найти длину периода, связанного со значением дискретного логарифма, $(-1, x)$.

В ранее описанных постквантовых схемах ЭЦП [16—18] использована вычислительная сложность СЗДЛ, заданной в КНАА, имеющих размерность $m = 4$ или 6 и содержащих достаточно большое число изоморфных циклических групп. Для вычисления открытого ключа выбирают циклическую группу, порядок которой равен простому числу. В этой группе выбирают элемент N и вычисляют значение N^x. Затем формируют две согласованные секретные маскирующие операции, ψ_1 и ψ_2, каждая из которых является взаимно коммутативной с операцией экспоненцирования, и вычисляют значения $Y = \psi_1(N^x)$ и $Z = \psi_2(N)$, принадлежащие двум разным циклическим группам, отличным от циклической группы, генерируемой элементом N. Периодическая функция $f(i, j) = Y^i Z^j$ содержит период длины $(-1, x)$, однако принимает произвольные значения в КНАА, которые не ограничены какой-то одной циклической группой. Это обусловливает стойкость схем ЭЦП, основанных на СЗДЛ, к атакам и использованием известных алгоритмов нахождения длины периода на квантовом компьютере.

При разработке протоколов открытого распределения ключей возможность использования скрытой циклической группы, в которой выполняется базовая операция экспоненцирования, отсутствует. Это связано с тем, что для обеспечения корректности работы криптосхем такого типа различные пользователи должны применять одну и ту же базовую циклическую группу.

Предложен способ построения криптосхем открытого распределения ключей, в котором использованы две различные маскирующие операции, выполняемые над секретным элементом N^x базовой циклической группы, заданной элементом N, являющимся общим параметром криптосхемы.

Алгебраический носитель криптосхемы

В качестве носителя схемы открытого распределения ключей, основанной на СЗДЛ, использо-

вана четырехмерная КНАА, заданная над простым конечным полем $GF(p)$ с помощью таблицы умножения базисных векторов (ТУБВ), представленной как таблица, содержащая глобальную двухстороннюю единицу. Операцию умножения векторов $\mathbf{A}=(a_0, a_1, a_2, a_3)$ и $\mathbf{B}=(b_0, b_1, b_2, b_3)$ выполняют по формуле

$$\mathbf{A}\circ\mathbf{B}=\sum_{i=0}^{3}\sum_{j=0}^{3} a_i b_j\left(\mathbf{e}_i\circ\mathbf{e}_j\right),$$

где произведение всевозможных пар базисных векторов заменяют на некоторый базисный вектор или однокомпонентный вектор. Умножение вектора **A** на скаляр λ выполняют по формуле $\lambda\mathbf{A}=(\lambda a_0, \lambda a_1, \lambda a_2, \lambda a_3)$, т. е. оно представляет собой λ-кратное сложение вектора **A**.

Задание четырехмерной КНАА с глобальной двухсторонней единицей $(0, 1, \lambda^{-1}, 0)$, где $\lambda\neq 0$

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\mathbf{e}_0$	0	$\mu\mathbf{e}_2$
$\mathbf{e}_1$	0	$\mathbf{e}_1$	0	$\mathbf{e}_3$
$\mathbf{e}_2$	$\lambda\mathbf{e}_0$	0	$\lambda\mathbf{e}_2$	0
$\mathbf{e}_3$	$\lambda\mu\mathbf{e}_1$	0	$\lambda\mathbf{e}_3$	0

При задании новых версий СЗДЛ и построении протоколов ЭЦП используют единичные элементы различных типов, содержащиеся в КНАА, используемых в качестве носителей криптосхем. В рассматриваемой здесь алгебре существует большое множество локальных левосторонних, правосторонних и двухсторонних единиц при наличии единственной глобальной двухсторонней единицы. Для вывода формулы для вычисления этой единицы рассмотрим решения векторных уравнений

$$\mathbf{X}\circ\mathbf{A}=\mathbf{A}; \quad (1)$$

$$\mathbf{A}\circ\mathbf{X}=\mathbf{A}, \quad (2)$$

где $\mathbf{A}=(a_0, a_1, a_2, a_3)$ — некоторый заданный четырехмерный вектор. Первое из этих двух уравнений сводится к следующей системе из четырех линейных уравнений с четырьмя неизвестными (x_0, x_1, x_2, x_3):

$$\begin{cases} x_0a_1+\lambda x_2a_0=a_0;\\ x_1a_1+\lambda\mu x_3a_0=a_1;\\ \mu x_0a_3+\lambda x_2a_2=a_2;\\ x_1a_3+\lambda x_3a_2=a_3. \end{cases} \quad (3)$$

Система (3) имеет единственное решение, $\mathbf{X}=(x_0, x_1, x_2, x_3)=(0, 1, \lambda^{-1}, 0)$, если выполняется условие $\mu a_0a_3\neq a_1a_2$. При этом указанное решение не зависит от координат вектора **A** и удовлетворяет системе (3) также и в случае $\mu a_0a_3=a_1a_2$, т. е. оно представляет собой глобальную левостороннюю единицу. Второе из упомянутых двух векторных уравнений сводится к следующей системе из четырех линейных уравнений с четырьмя неизвестными (x_0, x_1, x_2, x_3):

$$\begin{cases} a_0x_1+\lambda a_2x_0=a_0;\\ a_1x_1+\lambda\mu a_3x_0=a_1;\\ \mu a_0x_3+\lambda a_2x_2=a_2;\\ a_1x_3+\lambda a_3x_2=a_3. \end{cases} \quad (4)$$

Система (4) имеет решение $\mathbf{X}=(x_0, x_1, x_2, x_3)=(0, 1, \lambda^{-1}, 0)$, совпадающее с решением системы (3). Это решение не зависит от координат a_0, a_1, a_2, a_3 и является единственным при условии $\mu a_0a_3\neq a_1a_2$. Таким образом, вектор $\mathbf{E}=(0, 1, \lambda^{-1}, 0)$ является глобальной двухсторонней единицей рассматриваемой алгебры.

Легко показать, что для векторов $\mathbf{A}=(a_0, a_1, a_2, a_3)$, координаты которых удовлетворяют условию $\mu a_0a_3\neq a_1a_2$, каждое из двух следующих векторных уравнений:

$$\mathbf{X}\circ\mathbf{A}=\mathbf{E}; \quad (5)$$

$$\mathbf{A}\circ\mathbf{X}=\mathbf{E}, \quad (6)$$

имеет единственное решение. При этом решение (5) совпадает с решением (6), т. е. это решение представляет собой вектор $\mathbf{A}^{-1}$, являющийся обратным вектору **A**. В случае

$$\mu a_0a_3\neq a_1a_2 \quad (7)$$

векторные уравнения (5) и (6) не имеют других решений, т. е. неравенство (7) представляет собой условие обратимости вектора **A**. Условием необратимости вектора **A** является равенство

$$\mu a_0a_3=a_1a_2. \quad (8)$$

Используя (8), легко показать, что число необратимых векторов равно p^3+p^2-p, а число обратимых — $\Omega=p(p-1)(p^2-1)$. Как уже упоминалось, системы (3) и (4) для необратимых векторов имеют много различных решений. Эти решения представляют собой левосторонние и правосторонние локальные единицы соответственно. Локальными единицами называют векторы, которые действуют как единицы в рамках некоторых подмножеств элементов алгебры.

Локальные единицы и их типы

Пусть задан необратимый вектор $\mathbf{N} = (n_0, n_1, n_2, n_3)$. Для вычисления всех его локальных левосторонних единиц представим систему (3) в виде двух независимых систем из двух линейных уравнений:

$$\begin{cases} x_0 n_1 + \lambda x_2 n_0 = n_0; \\ \mu x_0 n_3 + \lambda x_2 n_2 = n_2; \end{cases} \quad (9)$$

$$\begin{cases} x_1 n_1 + \lambda\mu x_3 n_0 = n_1; \\ x_1 n_3 + \lambda x_3 n_2 = n_3. \end{cases} \quad (10)$$

Главный определитель системы (9) равен

$$\Delta = \begin{vmatrix} n_1 & \lambda n_0 \\ \mu n_3 & \lambda n_2 \end{vmatrix} = \lambda\left(n_1 n_2 - \mu n_0 n_3\right) = 0.$$

Вспомогательные определители равны

$$\Delta_0 = \begin{vmatrix} n_0 & \lambda n_0 \\ n_2 & \lambda n_2 \end{vmatrix} = \lambda n_0 n_2 - \lambda n_0 n_2 = 0;$$

$$\Delta_2 = \begin{vmatrix} n_1 & n_0 \\ \mu n_3 & n_2 \end{vmatrix} = n_1 n_2 - \mu n_0 n_3 = 0.$$

Таким образом, в системе (9) линейные уравнения зависимы и имеется p различных решений, для которых легко получить следующую формулу:

$$x_2 = \lambda^{-1} - \left(\lambda n_0\right)^{-1} n_1 x_0, \quad x_0 = 0, 1, ..., p-1. \quad (11)$$

Главный определитель системы (10) равен

$$\Delta = \begin{vmatrix} n_1 & \lambda\mu n_0 \\ n_3 & \lambda n_2 \end{vmatrix} = \lambda\left(n_1 n_2 - \mu n_0 n_3\right) = 0.$$

Вспомогательные определители равны

$$\Delta_0 = \begin{vmatrix} n_1 & \lambda\mu n_0 \\ n_3 & \lambda n_2 \end{vmatrix} = \lambda n_1 n_2 - \lambda\mu n_0 n_3 = 0;$$

$$\Delta_2 = \begin{vmatrix} n_1 & n_1 \\ n_3 & n_3 \end{vmatrix} = n_1 n_3 - n_1 n_3 = 0.$$

Таким образом, в системе (10) линейные уравнения зависимы и имеется p различных решений, для которых легко получить следующую формулу:

$$x_3 = \left(\lambda n_2\right)^{-1} n_3 - \left(\lambda n_2\right)^{-1} n_3 x_1, \quad x_1 = 0, 1, ..., p-1. \quad (12)$$

Объединяя (11) и (12), получаем формулу, описывающую p^2 различных локальных левосторонних единиц, связанных с необратимым вектором **N**:

$$\mathbf{L_N} = \left(d,\ h,\ \frac{1}{\lambda} - \frac{n_1}{\lambda n_0} d,\ \frac{n_3}{\lambda n_2} - \frac{n_3}{\lambda n_2} h \right), \quad d, h = 0, 1, ..., p-1. \quad (13)$$

В общем случае различным необратимым векторам соответствуют различные множества локальных единиц. Множество векторов (13) представляет собой локальные левосторонние единицы, действующие на множестве векторов, равных всевозможным линейным комбинациям всевозможных степеней вектора **N**.

Для вычисления всех локальных правосторонних единиц вектора $\mathbf{N} = (n_0, n_1, n_2, n_3)$ представим систему (4) в виде двух независимых систем из двух линейных уравнений:

$$\begin{cases} n_0 x_1 + \lambda n_2 x_0 = n_0; \\ n_1 x_1 + \lambda\mu n_3 x_0 = n_1; \end{cases} \quad (14)$$

$$\begin{cases} \mu n_0 x_3 + \lambda n_2 x_2 = n_2; \\ n_1 x_3 + \lambda n_3 x_2 = n_3. \end{cases} \quad (15)$$

Главный определитель системы (14) равен

$$\Delta = \begin{vmatrix} n_0 & \lambda n_2 \\ n_1 & \lambda\mu n_3 \end{vmatrix} = \lambda\left(\mu n_0 n_3 - n_1 n_2\right) = 0.$$

Вспомогательные определители равны

$$\Delta_0 = \begin{vmatrix} n_0 & \lambda n_2 \\ n_1 & \lambda\mu n_3 \end{vmatrix} = \lambda\left(\mu n_0 n_3 - n_1 n_2\right) = 0;$$

$$\Delta_2 = \begin{vmatrix} n_0 & n_0 \\ n_1 & n_1 \end{vmatrix} = 0.$$

Таким образом, в системе (14) линейные уравнения зависимы и имеется p различных решений, для которых легко получить следующую формулу:

$$x_1 = 1 - \lambda n_2 x_0 / n_0, \quad x_0 = 0, 1, ..., p-1. \quad (16)$$

Главный определитель системы (15) равен

$$\Delta = \begin{vmatrix} \mu n_0 & \lambda n_2 \\ n_1 & \lambda n_3 \end{vmatrix} = \lambda\left(\mu n_0 n_3 - n_1 n_2\right) = 0.$$

Вспомогательные определители равны

$$\Delta_0 = \begin{vmatrix} n_2 & \lambda n_2 \\ n_3 & \lambda n_3 \end{vmatrix} = \lambda n_2 n_3 - \lambda n_2 n_3 = 0;$$

$$\Delta_2 = \begin{vmatrix} \mu n_0 & n_2 \\ n_1 & n_3 \end{vmatrix} = \mu n_0 n_3 - n_1 n_2 = 0.$$

Таким образом, в системе (15) линейные уравнения зависимы и имеется p различных решений, для которых легко получить следующую формулу:

$$x_3 = n_3/n_1 - \lambda n_3 x_2/n_1, \quad x_2 = 0, 1, ..., p-1. \quad (17)$$

Объединяя (16) и (17), получаем формулу, описывающую p^2 различных локальных правосторонних единиц, связанных с необратимым вектором **N**:

$$\mathbf{R_N} = \left(d,\ 1 - \frac{\lambda n_2}{n_0} d,\ h,\ \frac{n_3}{n_1} - \frac{\lambda n_3}{n_1} d \right), \quad (18)$$
$$d, h = 0, 1, ..., p-1.$$

В общем случае различным необратимым векторам соответствуют различные множества локальных единиц. Множество векторов (18) представляет собой локальные правосторонние единицы, действующие на множестве векторов, равных всевозможным линейным комбинациям всевозможных степеней вектора **N**.

Множество локальных двухсторонних единиц, соответствующих вектору **N**, можно найти как пересечение множеств (13) и (18), что дает следующую формулу, описывающую p различных локальных двухсторонних единиц, действующих на множестве векторов, равных всевозможным линейным комбинациям всевозможных степеней вектора **N**:

$$\mathbf{E_N} = \left(d,\ 1 - \frac{\lambda n_2}{n_0} d,\ \frac{1}{\lambda} - \frac{n_1}{\lambda n_0} d,\ \frac{n_3}{n_0} d \right), \quad (19)$$
$$d = 0, 1, ..., p-1.$$

Заметим, что под локальными единичными элементами понимают не только элементы, принадлежащие рассматриваемому подмножеству элементов алгебры, но также элементы, которые не принадлежат этому подмножеству. Преобладающее число векторов, входящих в множества локальных единиц (13), (18) и (19), являются обратимыми векторами. Так, в (19) входит только один необратимый вектор, а в каждом из множеств (13) и (18) содержится p необратимых векторов и $p^2 - p$ обратимых.

Утверждение 1. Множество всевозможных линейных комбинаций всевозможных степеней обратимого вектора **A** является коммутативной подалгеброй рассматриваемой алгебры.

Доказательство. Сумма двух линейных комбинаций всевозможных степеней вектора **A** также является линейной комбинацией его степеней. Следовательно, операция сложения векторов в рассматриваемом множестве является замкнутой. Произведение двух линейных комбинаций всевозможных степеней вектора **A** также является линейной комбинацией его степеней. Следовательно, операция умножения векторов в рассматриваемом множестве является замкнутой. Докажем коммутативность операции умножения в рассматриваемом множестве векторов. Пусть $\mathbf{V}_1 = \sum_{i=0}^{w} \lambda_i \mathbf{A}^{s_i}$ и $\mathbf{V}_2 = \sum_{j=0}^{z} \mu_j \mathbf{A}^{t_j}$, где λ_i и μ_j — скалярные множители. Тогда имеем $\mathbf{V}_1 \circ \mathbf{V}_2 = \sum_{i,j=0}^{w,z} \lambda_i \mu_j \mathbf{A}^{s_i} \circ \mathbf{A}^{t_j} =$ $= \sum_{i,j=0}^{w,z} \lambda_i \mu_j \mathbf{A}^{s_i + t_j}$ и $\mathbf{V}_2 \circ \mathbf{V}_1 = \sum_{i,j=0}^{w,z} \lambda_i \mu_j \mathbf{A}^{t_i} \circ \mathbf{A}^{s_j} =$ $= \sum_{i,j=0}^{w,z} \lambda_i \mu_j \mathbf{A}^{t_j + s_i}$, т. е. $\mathbf{V}_1 \circ \mathbf{V}_2 = \mathbf{V}_2 \circ \mathbf{V}_1$.

Утверждение 2. Каждый из векторов, принадлежащих множествам (13), (18) и (19), является соответствующим (левосторонним, правосторонним или двухсторонним) локальным единичным элементом на множестве всевозможных линейных комбинаций всевозможных степеней необратимого вектора **N**.

Доказательство. Пусть $\mathbf{V} = \sum_{i=0}^{w} \lambda_i \mathbf{N}^{s_i}$ и $\mathbf{E_N}$ — элемент из множества (19). Имеем $\mathbf{V} \circ \mathbf{E_N} = \sum_{i=0}^{w} \lambda_i \left(\mathbf{N}^{s_i} \circ \mathbf{E_N} \right) = \sum_{i=0}^{w} \lambda_i \mathbf{N}^{s_i} = \mathbf{V}$ и $\mathbf{E_N} \circ \mathbf{V} = \sum_{i=0}^{w} \lambda_i \left(\mathbf{E_N} \circ \mathbf{N} \right)^{s_i} = \sum_{i=0}^{w} \lambda_i \mathbf{N}^{s_i} = \mathbf{V}$, т. е. $\mathbf{E_N}$ является локальной двухсторонней единицей на рассматриваемом множестве линейных комбинаций степеней вектора **N**. Аналогично выполняется доказательство для любой локальной единицы из множества (13) и множества (18).

Утверждение 3. Множество всевозможных линейных комбинаций всевозможных степеней необратимого вектора **N** не содержит обратимых векторов.

Доказательство. На обратимый вектор действует как единица единственный вектор — глобальная двухсторонняя единица, тогда как на любую линейную комбинацию степеней необратимого вектора **N** действуют как единицы многочисленные векторы из множеств (13), (18) и (19).

Найдем формулу для вычисления необратимого вектора $\mathbf{E}_{\mathbf{N}}^{*}$, являющегося локальной двухсторонней единицей на множестве линейных комбинаций степеней вектора **N**. Для этого вычислим в (19) такое значение d, при котором выполняется условие необратимости вектора:

$$d\left(\frac{n_3}{n_0}d\right)=\left(1-\frac{\lambda n_2}{n_0}d\right)\left(\frac{1}{\lambda}-\frac{n_1}{\lambda n_0}d\right).$$

Из последнего равенства получаем

$$d=\frac{n_0}{n_1+\lambda n_2}.$$

Подставляя полученное значение вместо d в (19), имеем

$$\mathbf{E}_{\mathbf{N}}^{*}=\begin{pmatrix}\dfrac{n_0}{n_1+\lambda n_2}, & 1-\dfrac{\lambda n_2}{n_1+\lambda n_2},\\ \dfrac{1}{\lambda}-\dfrac{n_1}{\lambda n_1+\lambda^2 n_2}, & \dfrac{n_3}{n_1+\lambda n_2}\end{pmatrix}. \qquad (20)$$

Вектор $\mathbf{E}_{\mathbf{N}}^{*}$ является единицей в конечной циклической группе, генерируемой необратимым вектором **N**. Пусть порядок этой группы равен ω (локальный порядок вектора **N**). Тогда значение может быть вычислено также и по формуле $\mathbf{E}_{\mathbf{N}}^{*}=\mathbf{N}^{\omega}$.

Генерация параметров криптосхемы

В качестве характеристики поля, над которым задается рассмотренная четырехмерная КНАА, выберем значение $p = 2q + 1$, где q — 256-битовое простое число. Сгенерируем необратимый вектор **N**, имеющий значение локального порядка q, и случайную локальную левостороннюю единицу **L**, относящуюся к вектору **N**, такую, что она является обратимым вектором порядка $p - 1$ и выполняется условие $\mathbf{L}\circ\mathbf{N}\neq\mathbf{N}\circ\mathbf{L}$.

Генерируя случайные параметры λ_1, λ_2, λ_3, s_1, s_2, s_3, сформируем обратимый вектор

$$\mathbf{Q}=\lambda_1\mathbf{L}^{s_1}+\lambda_2\mathbf{L}^{s_2}+\lambda_3\mathbf{L}^{s_3},$$

такой, что его порядок равен $p - 1$ и выполняется условие $\mathbf{Q}\circ\mathbf{N}\neq\mathbf{N}\circ\mathbf{Q}$.

Необратимый вектор **N** будет использован в качестве генератора базовой циклической группы, в которой будет выполнена операция возведения в степень, равную секретному ключу пользователя, при формировании его открытого ключа.

Обратимые векторы **Q** и **L** будут использованы для задания двух независимых маскирующих операций, зависящих от секретного ключа пользователя. Учитывая описанную процедуру генерации векторов **Q** и **L** и утверждение 1, можно сделать вывод, что для произвольных степеней t и u выполняется условие $\mathbf{Q}^t\circ\mathbf{L}^u=\mathbf{L}^u\circ\mathbf{Q}^t$. Благодаря этому условию обеспечивается взаимная коммутативность двух применяемых маскирующих операций.

Векторы **N**, **L** и **Q** и значения простых чисел p и q являются общими параметрами предлагаемой постквантовой схемы открытого распределения ключей.

Личным секретным ключом пользователя является тройка равновероятных случайных чисел (x, t, u), меньших, чем значение q. По своему личному секретному ключу пользователь вычисляет открытый ключ **Y** в соответствии со следующей формулой:

$$\mathbf{Y}=\mathbf{Q}^t\circ\mathbf{N}^x\circ\mathbf{L}^u\circ\mathbf{Q}^{-t}.$$

При формировании открытого ключа используют две маскирующие операции, зависящие от секретного ключа. Первая операция — это умножение вектора $\mathbf{N}^x$ на локальную левостороннюю единицу $\mathbf{L}^u$ справа, вторая — умножение слева на вектор $\mathbf{Q}^t$ и умножение справа на вектор $\mathbf{Q}^{-t}$. Для корректности работы схемы открытого распределения ключей требуется наличие свойств взаимной коммутативности этих двух маскирующих операций между собой и взаимной коммутативности каждой из них с базовой операцией возведения в степень.

Взаимная коммутативность двух маскирующих операций обеспечивается за счет перестановочности векторов **L** и **Q**. Взаимная коммутативность первой маскирующей операции с операцией возведения в степень выражается следующей формулой, справедливость которой легко доказать:

$$\left(\mathbf{N}\circ\mathbf{L}^u\right)^x=\mathbf{N}^x\circ\mathbf{L}^u.$$

Взаимная коммутативность второй маскирующей операции с операцией возведения в степень выражается следующей формулой, справедливость которой также легко доказать:

$$\left(\mathbf{Q}^t\circ\left(\mathbf{N}\circ\mathbf{L}^u\right)\circ\mathbf{Q}^{-t}\right)^x=\mathbf{Q}^t\circ\left(\mathbf{N}\circ\mathbf{L}^u\right)^x\circ\mathbf{Q}^{-t}.$$

Схема открытого распределения ключей

Пусть два удаленных пользователя имеют личные секретные ключи (x_1, t_1, u_1) и (x_2, t_2, u_2) и яв-

ляются владельцами открытых ключей $\mathbf{Y}_1$ и $\mathbf{Y}_2$ соответственно. В частности, они могут быть абонентами одного и того же удостоверяющего центра, выдавшего им цифровые сертификаты, с помощью которых каждый из них может подтвердить подлинность своего открытого ключа. Взаимодействуя по открытому каналу, они обмениваются цифровыми сертификатами, после чего вычисляют общий секретный ключ в виде четырехмерного вектора $\mathbf{Z}$.

Первый пользователь, используя открытый ключ $\mathbf{Y}_2$ второго пользователя, вычисляет значение

$$\mathbf{Z}_1 = \mathbf{Q}^{t_1} \circ \mathbf{Y}_2^{x_1} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_1}.$$

Второй пользователь, используя открытый ключ $\mathbf{Y}_1$ первого пользователя, вычисляет значение

$$\mathbf{Z}_2 = \mathbf{Q}^{t_2} \circ \mathbf{Y}_1^{x_2} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_2}.$$

Докажем корректность предложенной схемы открытого распределения ключей, т. е. выполнение равенства $\mathbf{Z}_1 = \mathbf{Z}_2$:

$$\begin{aligned}
\mathbf{Z}_1 &= \mathbf{Q}^{t_1} \circ \mathbf{Y}_2^{x_1} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_1} = \\
&= \mathbf{Q}^{t_1} \circ \left(\mathbf{Q}^{t_2} \circ \mathbf{N}^{x_2} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_2}\right)^{x_1} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_1} = \\
&= \mathbf{Q}^{t_1} \circ \mathbf{Q}^{t_2} \circ \left(\mathbf{N}^{x_2} \circ \mathbf{L}^{u_2}\right)^{x_1} \circ \mathbf{Q}^{-t_2} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_1} = \\
&= \mathbf{Q}^{t_2+t_1} \circ \mathbf{N}^{x_2 x_1} \circ \mathbf{L}^{u_2} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_2} \circ \mathbf{Q}^{-t_1} = \\
&= \mathbf{Q}^{t_2+t_1} \circ \mathbf{N}^{x_2 x_1} \circ \mathbf{L}^{u_2+u_1} \circ \mathbf{Q}^{-t_2-t_1};
\end{aligned}$$

$$\begin{aligned}
\mathbf{Z}_2 &= \mathbf{Q}^{t_2} \circ \mathbf{Y}_1^{x_2} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_2} = \\
&= \mathbf{Q}^{t_2} \circ \left(\mathbf{Q}^{t_1} \circ \mathbf{N}^{x_1} \circ \mathbf{L}^{u_1} \circ \mathbf{Q}^{-t_1}\right)^{x_2} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_2} = \\
&= \mathbf{Q}^{t_2} \circ \mathbf{Q}^{t_1} \circ \left(\mathbf{N}^{x_1} \circ \mathbf{L}^{u_1}\right)^{x_2} \circ \mathbf{Q}^{-t_1} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_2} = \\
&= \mathbf{Q}^{t_2} \circ \mathrm{Q}^{t_1} \circ \mathbf{N}^{x_1 x_2} \circ \mathbf{L}^{u_1} \circ \mathbf{L}^{u_2} \circ \mathbf{Q}^{-t_1} \circ \mathbf{Q}^{-t_2} = \\
&= \mathbf{Q}^{t_1+t_2} \circ \mathbf{N}^{x_1 x_2} \circ \mathbf{L}^{u_1+u_2} \circ \mathbf{Q}^{-t_1+t_2} = \mathbf{Z}_1.
\end{aligned}$$

Заключение

Предложена новая четырехмерная КНАА с глобальной двухсторонней единицей, изучены ее свойства. Разработана новая форма СЗДЛ для реализации протоколов открытого распределения ключей, отличающаяся использованием двух маскирующих операций, обладающих свойством взаимной коммутативности. Предложенная криптосхема представляет интерес как постквантовый протокол открытого распределения ключей.

В качестве альтернативных алгебраических носителей предложенной постквантовой криптосхемы могут быть использованы четырехмерные КНАА с глобальной двухсторонней единицей, для которых получены формулы, описывающие множества локальных единиц [19, 20].

Литература

1. Proceedings of the 7th International Workshop on Post-Quantum Cryptography, PQCrypto 2016. Fukuoka, Japan, February 24—26, 2016. [Электронный ресурс]. Режим доступа: Lecture Notes in Computer Science (LNCS) series. — Springer, 2016. V. 9606. — 270 p.
2. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. Режим доступа: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf
3. Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9—11, 2018, Proceedings. Lecture Notes in Computer Science series. — Springer, 2018. V. 10786.
4. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.
5. *Yan S. Y.* Quantum Computational Number Theory. — Springer, 2015. — 252 p.
6. *Yan S. Y.* Quantum Attacks on Public-Key Cryptosystems. — Springer, 2014. — 207 p.
7. Post-Quantum Cryptography: Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019 // Lecture Notes in Computer Sci. 2019. V. 11505. — 420 p.
8. *Moldovyan D. N.* Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. V. 18. P. 165—176.
9. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.
10. *Moldovyan D. N.* A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. № 2. P. 293—308.
11. *Ekert A., Jozsa R.* Quantum computation and Shor's factoring algorithm // Rev. Mod. Phys. 1996. V. 68. P. 733.
12. *Jozsa R.* Quantum algorithms and the fourier transform // Proc. Roy. Soc. London Ser A. 1998. V. 454. P. 323—337.
13. *Глухов М. М.* К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 5—22.
14. *Кузьмин А. С., Марков В. Т., Михалев А. А., Михалев А. В., Нечаев А. А.* Криптографические алгоритмы на группах и алгебрах // Фундаментальная и прикладная математика. 2015. Т. 20. № 1. С. 205—222.
15. *Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.* Cryptographic Algorithms on Groups and Algebras // J. Math. Sci. 2017. V. 223. № 5. P. 629—641.
16. *Moldovyan A. A., Moldovyan N. A.* Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science J. Moldova. 2018. V. 26. № 3(78). P. 301—313.
17. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дис-

кретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.

18. *Moldovyan N. A.* Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2019. № 1(89). P. 71—78.

19. *Абросимов И. К., Ковалева И. В., Молдовян Н. А.* Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3—13.

20. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.

Post-quantum scheme of the public key distribution

D. N. Moldovyan, A. A. Moldovyan

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia

A new method for the public key distribution is proposed. The method is based on the hidden discrete logarithm problem set in a finite non-commutative associative algebra with the two-sided global unit and is characterized in applying two different mutually commutative operations which mask the basic exponentiation operation in a cyclic group of sufficiently large prime order. A cryptoscheme using the finite algebra, containing a large set of the left-sided units described by a mathematical formula, as its algebraic support and implementing the method is introduced. The developed cryptoscheme represents interest for constructing post-quantum public key distribution protocols.

Keywords: information protection, cryptography, public key distribution, discrete logarithm problem, finite associative algebra, non-commutative algebra, global unit, local unit, left-sided unit.

Bibliography — 20 references. *Received January 19, 2020*

УДК 003

Способы задания некоммутативных алгебр как носителей постквантовых криптосхем

Р. Ш. Фахрутдинов, канд. техн. наук; *А. Ю. Мирин*, канд. техн. наук; *И. К. Абросимов*
ФГБУН «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, Россия

В рамках развития обобщенных способов задания конечных некоммутативных ассоциативных алгебр различной размерности для использования в качестве алгебраических носителей постквантовых двухключевых криптосхем, основанных на скрытой задаче дискретного логарифмирования, предложен новый унифицированный способ задания алгебр указанного типа и рассмотрено применение ранее известного метода вложения для построения четырехмерных и восьмимерных алгебр. Показано, что метод вложения позволяет получить восьмимерные алгебры с операцией векторного умножения, которая имеет более низкую вычислительную сложность, тогда как новый способ имеет преимущества при задании четырехмерных алгебр.

Ключевые слова: постквантовая криптография, конечные некоммутативные алгебры, конечные ассоциативные алгебры, локальные единицы.

Одним из перспективных направлений построения практичных постквантовых криптосхем с открытым ключом является использование вычислительной трудности скрытой задачи дискретного логарифмирования (СЗДЛ) [1, 2]. На основе СЗДЛ предложены алгоритмы электронной цифровой подписи (ЭЦП) [3, 4], открытого согласования ключа [5, 6] и коммутативного шифрования [7, 8]. Алгебраический носитель таких криптосхем представляет собой конечную некоммутативную ассоциативную алгебру (КНАА). Известно и исследовано ограниченное число таких алгебр, тогда как для построения различных постквантовых двухключевых криптосхем используют КНАА, обладающие различными свойствами.

В целях расширения класса потенциальных алгебраических носителей в работах [9, 10] предложены унифицированные способы задания КНАА, которые состоят в задании математической формулы, генерирующей так называемую таблицу умножения базисных векторов, которая задает некоммутативную ассоциативную операцию векторного умножения элементов конечного векторного пространства. Данная формула в качестве параметра включает размерность векторного пространства, что позволяет построить некоторый класс КНАА, включающий алгебры различных размерностей. Тем не менее класс КНАА, задаваемый по некоторой унифицированной математической формуле, задает только одну алгебру для фиксированного значения размерности. Поэтому остается задача построения различных КНАА заданной размерности. Это делает актуальным расширение ряда унифицированных способов задания КНАА, а также разработку других способов задания новых алгебр.

Авторы предлагают новый способ унифицированного задания КНАА. Проведено его сравнение со способом построения КНАА методом вложения [11].

Фахрутдинов Роман Шафкатович, заведующий лабораторией.
E-mail: fahr@cobra.ru
Мирин Анатолий Юрьевич, старший научный сотрудник.
E-mail: mirin@cobra.ru
Абросимов Иван Константинович, младший научный сотрудник.
E-mail: ivnabr@yandex.ru

Статья поступила в редакцию 23 ноября 2020 г.

Задание конечных некоммутативных ассоциативных алгебр

Рассмотрим m-мерное векторное пространство, элементами которого являются всевозможные векторы вида

$$\mathbf{A} = (a_0, a_1, \ldots, a_{m-1}) = a_0\mathbf{e}_0 + a_1\mathbf{e}_1 + \ldots + a_{m-1}\mathbf{e}_{m-1},$$

где $a_i \in GF(p)$; p — простое число; $\mathbf{e}_i$ — формальные базисные векторы.

Дополнительно к стандартным операциям в векторном пространстве (операции сложения векторов и операции умножения вектора на скаляр) определим операцию умножения "$\circ$" векторов

$\mathbf{A}=\sum_{i=0}^{m-1}a_i\mathbf{e}_i$ и $\mathbf{B}=\sum_{j=0}^{m-1}b_j\mathbf{e}_j$ в соответствии со следующей формулой:

$$\mathbf{A}\circ\mathbf{B}=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}a_ib_j\mathbf{e}_i\circ\mathbf{e}_j, \qquad (1)$$

где каждое из всевозможных произведений пар базисных векторов заменяется на однокомпонентный вектор в соответствии с некоторым правилом, задаваемым в виде таблицы умножения базисных векторов (ТУБВ). Например, конечная алгебра кватернионов задается ТУБВ, которая представлена в виде табл. 1. Примем, что в произведении $\mathbf{e}_i\circ\mathbf{e}_j$ значение i задает строку, а значение j — столбец, на пересечении которых находится ячейка, содержащая значение этого произведения.

Таблица 1

Задание конечной алгебры кватернионов

$\circ$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$-\mathbf{e}_0$	$\mathbf{e}_3$	$-\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$-\mathbf{e}_3$	$-\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_2$	$-\mathbf{e}_1$	$-\mathbf{e}_0$

Векторное пространство с определенной таким образом операцией умножения векторов, которая является дистрибутивной справа и слева, называют m-мерной алгеброй. Для построения криптосхем на основе СЗДЛ интерес представляют КНАА.

Рассмотрим произведение векторов **A**, **B** и $\mathbf{C}=\sum_{k=0}^{m-1}c_k\mathbf{e}_k$, осуществляемое с применением формулы (1) в соответствии со следующими двумя вариантами:

$$(\mathbf{A}\circ\mathbf{B})\circ\mathbf{C}=\left(\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}a_ib_j\mathbf{e}_i\circ\mathbf{e}_j\right)\circ\sum_{k=0}^{m-1}c_k\mathbf{e}_k= \qquad (2)$$
$$=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1}a_ib_jc_k(\mathbf{e}_i\circ\mathbf{e}_j)\circ\mathbf{e}_k;$$

$$\mathbf{A}\circ(\mathbf{B}\circ\mathbf{C})=\left(\sum_{i=0}^{m-1}a_i\mathbf{e}_i\right)\circ\left(\sum_{j=0}^{m-1}\sum_{k=0}^{m-1}b_jc_k\mathbf{e}_i\circ\mathbf{e}_j\right)= \qquad (3)$$
$$=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\sum_{k=0}^{m-1}a_ib_jc_k\mathbf{e}_i\circ(\mathbf{e}_j\circ\mathbf{e}_k).$$

Равенство правых частей выражений (2) и (3) имеет место, если равенство

$$(\mathbf{e}_i\circ\mathbf{e}_j)\circ\mathbf{e}_k=\mathbf{e}_i\circ(\mathbf{e}_j\circ\mathbf{e}_k) \qquad (4)$$

имеет место для всех возможных троек значений (i, j, k).

Унифицированный способ задания конечных некоммутативных ассоциативных алгебр

Предлагаемый унифицированный способ задания КНАА произвольных четных размерностей $m \geq 4h$ (где h = 1, 2, 3, …) описывается следующей формулой для вычисления произведения пары базисных векторов $\mathbf{e}_i\circ\mathbf{e}_j$ при $i,\ j$ = 1, 2, 3, …, m – 1:

$$\mathbf{e}_i\circ\mathbf{e}_j=\begin{cases}\mathbf{e}_{i+j+m/2}, & \text{если } i \mod 2=0;\\ \mathbf{e}_{i-j+m/2}, & \text{если } i \mod 2=1,\end{cases} \qquad (5)$$

где операции сложения и вычитания выполняются по модулю m.

Докажем, что для ТУБВ, генерируемой формулой (5), равенство (4) выполняется для всех возможных значений троек индексов (i, j, k) при любом значении размерности m, кратном числу 4. Примем соглашение об обозначении четных значений индексов символами i, j, k, а нечетных — символами i', j', k' (со штрихом). Ясно, что четность индекса k не влияет на выбор формулы в правой части выражения (5), используемой для вычисления индекса результирующего базисного вектора. Поэтому достаточно проверить выполнимость указанного равенства (4) для следующих четырех случаев: $i,\ j$; $i,\ j'$; $i',\ j$; $i',\ j'$.

Случай 1 (i и j — четные значения):

$$\begin{cases}(\mathbf{e}_i\circ\mathbf{e}_j)\circ\mathbf{e}_k=\mathbf{e}_{i+j+m/2}\circ\mathbf{e}_k=\mathbf{e}_{i+j+k}\\ \mathbf{e}_i\circ(\mathbf{e}_j\circ\mathbf{e}_k)=\mathbf{e}_i\circ\mathbf{e}_{j+k+m/2}=\mathbf{e}_{i+j+k}\end{cases}\Rightarrow$$
$$\Rightarrow(\mathbf{e}_i\circ\mathbf{e}_j)\circ\mathbf{e}_k=\mathbf{e}_i\circ(\mathbf{e}_j\circ\mathbf{e}_k).$$

Случай 2 (i — четное, j' — нечетное):

$$\begin{cases}(\mathbf{e}_i\circ\mathbf{e}_{j'})\circ\mathbf{e}_k=\mathbf{e}_{i+j'+m/2}\circ\mathbf{e}_k=\mathbf{e}_{i+j'-k}\\ \mathbf{e}_i\circ(\mathbf{e}_{j'}\circ\mathbf{e}_k)=\mathbf{e}_i\circ\mathbf{e}_{j'-k+m/2}=\mathbf{e}_{i+j'-k}\end{cases}\Rightarrow$$
$$\Rightarrow(\mathbf{e}_i\circ\mathbf{e}_{j'})\circ\mathbf{e}_k=\mathbf{e}_i\circ(\mathbf{e}_{j'}\circ\mathbf{e}_k).$$

Случай 3 (i' — нечетное, j — четное):

$$\begin{cases}\left(\mathbf{e}_{i'}\circ\mathbf{e}_j\right)\circ\mathbf{e}_k=\mathbf{e}_{i'-j+m/2}\circ\mathbf{e}_k=\mathbf{e}_{i'-j-k}\\ \mathbf{e}_{i'}\circ\left(\mathbf{e}_j\circ\mathbf{e}_k\right)=\mathbf{e}_{i'}\circ\mathbf{e}_{j+k+m/2}=\mathbf{e}_{i'-j-k}\end{cases}\Rightarrow$$
$$\Rightarrow\left(\mathbf{e}_{i'}\circ\mathbf{e}_j\right)\circ\mathbf{e}_k=\mathbf{e}_{i'}\circ\left(\mathbf{e}_j\circ\mathbf{e}_k\right).$$

Случай 4 (i' и j' — нечетные значения):

$$\begin{cases}\left(\mathbf{e}_{i'}\circ\mathbf{e}_{j'}\right)\circ\mathbf{e}_k=\mathbf{e}_{i'-j'+m/2}\circ\mathbf{e}_k=\mathbf{e}_{i'-j'+k}\\ \mathbf{e}_{i'}\circ\left(\mathbf{e}_{j'}\circ\mathbf{e}_k\right)=\mathbf{e}_{i'}\circ\mathbf{e}_{j'-k+m/2}=\mathbf{e}_{i'-j'+k}\end{cases}\Rightarrow$$
$$\Rightarrow\left(\mathbf{e}_{i'}\circ\mathbf{e}_{j'}\right)\circ\mathbf{e}_k=\mathbf{e}_{i'}\circ\left(\mathbf{e}_{j'}\circ\mathbf{e}_k\right).$$

Таким образом, операция умножения векторов, задаваемая правилом, представленным в компактной аналитической форме (5), является ассоциативной, а при $h\ge 2$ ($m\ge 8$) также и некоммутативной. При $m = 4$ этот способ приводит к построению четырехмерной коммутативной ассоциативной алгебры, в которой умножение задано по табл. 2. Единицей такой алгебры является вектор (0010).

Таблица 2

Задание векторного умножения для случая $m = 4$

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_2$

По аналогии с табл. 1, в которой распределение базисных векторов является симметричным, а некоммутативность векторного умножения достигается несимметричным распределением структурного коэффициента, равного –1, при котором сохраняется свойство ассоциативности, табл. 2 можно преобразовать в табл. 3, задающую четырехмерную КНАА с глобальной двухсторонней единицей в виде вектора **E** = (0010). Возможны и другие виды несимметричного распределения коэффициента –1 по ячейкам табл. 2, при которых сохраняется свойство ассоциативности операции векторного умножения.

Таблица 3

Внесение несимметричного распределения структурного коэффициента, равного –1

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_2$	$-\mathbf{e}_3$	$\mathbf{e}_0$	$-\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_3$	$-\mathbf{e}_2$	$\mathbf{e}_1$	$-\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\mathbf{e}_2$

При $m = 8$ предложенный унифицированный способ приводит к построению восьмимерной КНАА, в которой умножение задано табл. 4.

Таблица 4

Задание векторного умножения для случая $m = 8$

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_7$	$\mathbf{e}_6$
$\mathbf{e}_2$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_3$	$\mathbf{e}_7$	$\mathbf{e}_6$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_4$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_5$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_7$	$\mathbf{e}_6$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_2$
$\mathbf{e}_6$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_7$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_7$	$\mathbf{e}_6$	$\mathbf{e}_5$	$\mathbf{e}_4$

Единицей такой алгебры является вектор **E** = (00001000). Для построения двухключевых криптосхем на основе СЗДЛ важным является наличие большого числа циклических групп большого простого порядка. Поэтому интересен вопрос о значениях мультипликативного порядка, которые могут иметь векторы как элементы различных КНАА. Выполнение большого числа вычислительных экспериментов показало, что в рассмотренных КНАА размерности $m = 4$ и 8 векторы имеют порядки, равные всевозможным делителям числа $p^2 - 1 = (p - 1)(p + 1)$, включая само это число. Для получения большого простого порядка векторов следует выбирать характеристику поля $GF(p)$, над которым задается КНАА в виде простого числа $p = 2q + 1$ или в виде простого числа $p = 2q - 1$, где q — 256-битное простое число. По каждой из этих формул нужное простое число p генерируют путем перебора с проверкой случайных простых значений q до тех пор, пока вычисляемое по выбранной формуле значение p не окажется простым.

Задание конечных некоммутативных ассоциативных алгебр методом вложения

Рассмотрим метод вложения, предложенный в работе [11]. Пусть имеется ТУБВ, задающая КНАА некоторой размерности, например $m = h$. Обозначим формальные базисные векторы следующим образом: $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_h$. Вводя вторую нумерацию в виде верхнего индекса для указанных базисных векторов, можно сформировать следующие k аналогичных ТУБВ: $\mathbf{T}^i$, $i = 1, 2, ..., k$. Таким образом, базисные векторы $\left\{\mathbf{v}_1^i, \mathbf{v}_2^i, ..., \mathbf{v}_h^i\right\}$ соответствуют таблице $\mathbf{T}^i$. Пусть рассматривае-

мые таблицы выбраны так, что в объединении всех множеств $\left\{\mathbf{v}_1^i, \mathbf{v}_2^i, ..., \mathbf{v}_h^i\right\}$, $i = 1, 2, ..., k$, все базисные векторы попарно различны. Достаточно очевидно, что если исходная ТУБВ задает ассоциативное векторное умножение векторов, то каждая отдельная таблица $\mathbf{T}^i$ также задает ассоциативное векторное умножение (на самом деле, они идентичны с точностью до обозначений).

Можно определить некоторый класс базисных векторов $\overline{\mathbf{v}_j}$ как множество базисных векторов $\left\{\mathbf{v}_j^1, \mathbf{v}_j^2, ..., \mathbf{v}_j^k\right\}$. Пусть такие классы выделены для $j = 1, 2, ..., h$. Также можно определить операцию умножения "$\bullet$" классов $\overline{\mathbf{v}_j}$ и $\overline{\mathbf{v}_g}$, где $j, g \in \{1, 2, ..., k\}$, по следующему правилу. Возьмем произвольное натуральное число $z \in \{1, 2, ..., k\}$, после чего из множества $\left\{\mathbf{v}_j^1, \mathbf{v}_j^2, ..., \mathbf{v}_j^k\right\}$ возьмем элемент $\mathbf{v}_j^z$, а из множества $\left\{\mathbf{v}_g^1, \mathbf{v}_g^2, ..., \mathbf{v}_g^k\right\}$ — элемент $\mathbf{v}_g^z$. Над базисными векторами $\mathbf{v}_j^z$ и $\mathbf{v}_g^z$, которые принадлежат одной и той же ТУБВ, выполним операцию векторного умножения по таблице $\mathbf{T}^z$, в результате чего получим $\mathbf{v}_j^z \circ \mathbf{v}_g^z = \mathbf{v}_q^z$, где базисный вектор в правой части задан таблицей $\mathbf{T}^z$. В качестве результата умножения классов $\overline{\mathbf{v}_j}$ и $\overline{\mathbf{v}_g}$ возьмем класс $\overline{\mathbf{v}_q}$, которому принадлежит базисный вектор $\mathbf{v}_q^z$, т. е. имеем $\overline{\mathbf{v}_j} \bullet \overline{\mathbf{v}_g} = \overline{\mathbf{v}_q}$. Очевидно, что по построению результат умножения классов не зависит от выбора значения $z \in \{1, 2, \ldots, k\}$.

Операция умножения "$*$" таблицы $\mathbf{T}^i$, $i = 1, 2, ..., k$, на скаляр $\lambda \in GF(p)$, где $GF(p)$ — поле, над которым задано рассматриваемое векторное пространство, определяется как процедура умножения на структурный коэффициент λ базисных векторов в каждой клетке $\mathbf{T}^i$ [11]. Последнее, очевидно, приводит к тому, что $\lambda\mathbf{T}^i$ уже не принадлежит множеству таблиц $\mathbf{T}^i$, $i = 1, 2, ..., k$.

Зададим над множеством $\left\{\mathbf{T}^1, \mathbf{T}^2, ..., \mathbf{T}^k\right\}$, табличную ассоциативную и коммутативную операцию умножения, результатом которой может быть таблица $\lambda\mathbf{T}^w$ при некотором значении $w \in \{1, 2, \ldots, k\}$. Обозначим таблицу умножения элементов множества $\left\{\mathbf{T}^1, \mathbf{T}^2, ..., \mathbf{T}^k\right\}$ как TABLE.

В работе [11] показано, что задавая детальное представление каждой ТУБВ в TABLE, получаем результирующую ТУБВ, определяющую ассоциативную операцию умножения "$\circ$" над следующим множеством базисных векторов:

$$\left\{\mathbf{v}_1^1, \mathbf{v}_2^1, ..., \mathbf{v}_h^1, \mathbf{v}_1^2, \mathbf{v}_2^2, ..., \mathbf{v}_h^2, ..., \mathbf{v}_1^k, \mathbf{v}_2^k, ..., \mathbf{v}_h^k\right\}.$$

При этом каждый элемент данного множества, например $\mathbf{v}_\mu^\varepsilon$, может быть однозначно задан как элемент, одновременно принадлежащий классу $\overline{\mathbf{v}_\mu}$ и таблице $\mathbf{T}^\varepsilon$: $\mathbf{v}_\mu^\varepsilon = \left(\overline{\mathbf{v}_\mu} \cap \mathbf{T}^\varepsilon\right)$, где "$\cap$" — операция нахождения элемента, принадлежащего одновременно двум множествам-операндам. Легко показать, что операция умножения базисных векторов $\mathbf{v}_\mu^\varepsilon$ и $\mathbf{v}_\psi^\tau = \left(\overline{\mathbf{v}_\psi} \cap \mathbf{T}^\tau\right)$ может быть выполнена по следующей формуле [11]:

$$\mathbf{v}_\mu^\varepsilon \circ \mathbf{v}_\psi^\tau = \left(\overline{\mathbf{v}_\mu} \cap \mathbf{T}^\varepsilon\right) \circ \left(\overline{\mathbf{v}_\psi} \cap \mathbf{T}^\tau\right) =$$

$$= \left(\left(\overline{\mathbf{v}_\mu} \bullet \overline{\mathbf{v}_\psi}\right) \cap \left(\mathbf{T}^\varepsilon * \mathbf{T}^\tau\right)\right).$$

Таким образом, выполнение операции над векторами размерности hk сводится к выполнению операций "$\bullet$", "$*$" и "$\cap$". Если операции "$\bullet$" и "$*$" ассоциативны, то операция умножения векторов размерности hk также является ассоциативной. Пусть даны три базисных вектора: $\mathbf{v}_\beta^\alpha$, $\mathbf{v}_\mu^\varepsilon$ и $\mathbf{v}_\psi^\tau$. Тогда имеем [11]

$$\left(\mathbf{v}_\beta^\alpha \circ \mathbf{v}_\mu^\varepsilon\right) \circ \mathbf{v}_\psi^\tau = \left(\left(\overline{\mathbf{v}_\beta} \bullet \overline{\mathbf{v}_\mu}\right) \cap \left(\mathbf{T}^\alpha * \mathbf{T}^\varepsilon\right)\right) \circ \left(\overline{\mathbf{v}_\psi} \cap \mathbf{T}^\tau\right) =$$

$$= \left(\left(\left(\overline{\mathbf{v}_\beta} \bullet \overline{\mathbf{v}_\mu}\right) \bullet \overline{\mathbf{v}_\psi}\right) \cap \left(\left(\mathbf{T}^\alpha * \mathbf{T}^\varepsilon\right) * \mathbf{T}^\tau\right)\right) =$$

$$= \left(\left(\overline{\mathbf{v}_\beta} \bullet \left(\overline{\mathbf{v}_\mu} \bullet \overline{\mathbf{v}_\psi}\right)\right) \cap \left(\mathbf{T}^\alpha * \left(\mathbf{T}^\varepsilon * \mathbf{T}^\tau\right)\right)\right) =$$

$$= \left(\overline{\mathbf{v}_\beta} \cap \mathbf{T}^\alpha\right) \circ \left(\left(\overline{\mathbf{v}_\mu} \bullet \overline{\mathbf{v}_\psi}\right) \cap \left(\mathbf{T}^\varepsilon * \mathbf{T}^\tau\right)\right) =$$

$$= \left(\overline{\mathbf{v}_\beta} \cap \mathbf{T}^\alpha\right) \circ \left(\left(\overline{\mathbf{v}_\mu} \cap \mathbf{T}^\varepsilon\right) \circ \left(\overline{\mathbf{v}_\psi} \cap \mathbf{T}^\tau\right)\right) = \mathbf{v}_\beta^\alpha \circ \left(\mathbf{v}_\mu^\varepsilon \circ \mathbf{v}_\psi^\tau\right).$$

т. е. ассоциативность операции "$\circ$" доказана.

Рассмотрим примеры построения ТУБВ с помощью описанного метода вложения. Используя некоторую известную некоммутативную ассоциативную ТУБВ для случая $m = 4$, например представленную в виде табл. 5 (см. работу [12]), и коммутативную ассоциативную ТУБВ для случая $m = 2$, представленную в виде табл. 6, в соответствии с методом вложения табл. 5 в табл. 6 получаем результирующую ТУБВ размерности $m = 8$

(табл. 7), задающую восьмимерную КНАА, в которой максимальный мультипликативный порядок элементов векторов равен $p^4 - 1$ в случае, если структурный коэффициент λ является квадратичным невычетом, и $p^2 - 1$, если структурный коэффициент λ является квадратичным вычетом. В построенной методом вложения КНАА единицей является вектор $\mathbf{E} = (10010000)$. При этом сложность операции умножения векторов уменьшается примерно в два раза за счет наличия в половине клеток ТУБВ структурного коэффициента, равного нулю.

Таблица 5

Задание векторного умножения в четырехмерной КНАА [13]

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0
$\mathbf{e}_1$	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$

Таблица 6

Задание векторного умножения в двухмерной коммутативной ассоциативной алгебре ($\lambda \neq 0$) [14]

○	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_0$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$

Таблица 7

Восьмимерная КНАА, построенная методом вложения

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0
$\mathbf{e}_1$	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	0	0	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	0	0
$\mathbf{e}_3$	0	0	$\mathbf{e}_2$	$\mathbf{e}_3$	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	0	0
$\mathbf{e}_5$	0	0	$\mathbf{e}_4$	$\mathbf{e}_5$	0	0	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_6$	$\mathbf{e}_6$	$\mathbf{e}_7$	0	0	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	0	0
$\mathbf{e}_7$	0	0	$\mathbf{e}_6$	$\mathbf{e}_7$	0	0	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$

В соответствии с методом вложения табл. 6 в табл. 5 получаем результирующую ТУБВ размерности $m = 8$ (табл. 8), задающую восьмимерную КНАА, в которой максимальный мультипликативный порядок элементов векторов, так же как и в предыдущем случае, равен $p^4 - 1$, если структурный коэффициент λ является квадратичным невычетом, и $p^2 - 1$, если структурный коэффициент λ является квадратичным вычетом. В построенной методом вложения второй КНАА единицей является вектор $\mathbf{E} = (10000010)$. При этом также получаем прореженную ТУБВ.

Таблица 8

Восьмимерная КНАА, построенная по альтернативному варианту применения метода вложения

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	0	0	0	0
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	0	0	0	0
$\mathbf{e}_2$	0	0	0	0	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	0	0	0	0	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$	0	0	0	0
$\mathbf{e}_5$	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$	0	0	0	0
$\mathbf{e}_6$	0	0	0	0	$\mathbf{e}_4$	$\mathbf{e}_5$	$\mathbf{e}_6$	$\mathbf{e}_7$
$\mathbf{e}_7$	0	0	0	0	$\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\mathbf{e}_7$	$\lambda\mathbf{e}_6$

Сравнение способов построения таблиц умножения базисных векторов

Выбор двухмерной и четырехмерной алгебр, операция умножения в последней из которых задана прореженной ТУБВ, и использование метода вложения ТУБВ алгебры большей размерности в ТУБВ алгебры меньшей размерности обеспечили построение восьмимерной прореженной ТУБВ, за счет чего обеспечивается двукратное уменьшение вычислительной сложности операции векторного умножения по сравнению с восьмимерной КНАА, заданной табл. 4. Описанный унифицированный способ задания ТУБВ не позволяет получить прореженные ТУБВ. Таким образом, метод вложения выгодно отличается тем, что он позволяет при наличии прореженных ТУБВ, задающих КНАА малой размерности, легко построить прореженные ТУБВ для задания КНАА увеличенной размерности (в два, три и более раза).

Минимальное значение разрядности КНАА, которую можно задать по предложенному унифицированному способу, равно $m = 4$. Такой же разрядности КНАА могут быть заданы и способом вложения. Действительно, в рассмотренную ТУБВ, задающую двухмерную коммутативную ассоциативную алгебру, можно вложить ТУБВ, задающую двухмерную КНАА, описанную в работе [14]. Это приводит к построению ТУБВ, представленной в табл. 9. Данная ТУБВ задает КНАА с множеством правосторонних глобальных единиц, для которой может быть указано гомоморфное отображение в двухмерную коммутативную алгебру, что не позволяет построенную таким образом четырехмерную КНАА использовать для построения криптосхем, основанных на СЗДЛ, поскольку СЗДЛ в такой алгебре легко сводится к обычной задаче дискретного логарифмирования в

явно заданной циклической группе. Предложенный унифицированный способ с дополнительным применением метода несимметричного распределения структурного коэффициента позволяет построить четырехмерные КНАА с глобальной двухсторонней единицей, которые пригодны для использования в качестве носителей СЗДЛ.

Таблица 9

Задание векторного умножения в четырехмерной КНАА, содержащей p^2 глобальных правосторонних единиц

○	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_2$	$\mathbf{e}_2$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_1$	$\mathbf{e}_3$	$\mathbf{e}_3$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_0$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_3$	$\mathbf{e}_1$	$\mathbf{e}_1$

Таким образом, с точки зрения построения четырехмерных КНАА для использования в качестве алгебраического носителя криптосхем, основанных на вычислительной сложности СЗДЛ, преимуществом обладает предложенный унифицированный способ построения ТУБВ.

Заключение

Предложен новый унифицированный способ задания КНАА, который дополняет известные способы унифицированного построения частных классов КНАА и расширяет возможности выбора КНАА с требуемыми свойствами для построения двухключевых криптосхем, основанных на вычислительной сложности СЗДЛ. Выполнено сравнение предложенного способа с заданием КНАА методом вложения, и показано, что каждый из указанных двух способов имеет свои особенности, которые могут быть использованы при разработке криптосхем.

Следует отметить способ преобразования симметричной ТУБВ в несимметричную ассоциативную ТУБВ за счет введения несимметричного распределения структурных коэффициентов. Несмотря на то что для сохранения свойства ассоциативности исходной ТУБВ требуется использовать структурный коэффициент, имеющий специальное значение, равное −1, этот способ, видимо, имеет более общее значение, чем продемонстрировано в данной работе. Представляет интерес использование метода несимметричного распределения структурного коэффициента для построения шестимерных и восьмимерных КНАА. Однако выбор соответствующей исходной симметричной ТУБВ для каждого из этих случаев и нахождение нужных распределений структурного коэффициента составляют самостоятельную задачу, включающую значительный объем экспериментальных исследований.

Литература

1. *Молдовян А. А., Молдовян Н. А.* Новые формы задания скрытой задачи дискретного логарифмирования // Тр. СПИИРАН. 2019. № 2(18). С. 504—529. DOI: 10.15622/sp.18.2.504-529
2. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81. DOI: 10.14529/mmp190106
3. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
4. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.
5. *Фахрутдинов Р. Ш., Мирин А. Ю., Молдовян Д. Н., Костина А. А.* Схемы открытого согласования ключей на основе скрытой задачи дискретного логарифмирования // Информационные технологии. 2020. Т. 26. № 10. С. 577—585. DOI: 10.17587/it.26. 577-585
6. *Moldovyan D. N.* Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V. 27. № 1(79). P. 56—72.
7. *Молдовяну П. А., Морозова Е. В., Молдовян Д. Н., Пилькевич С. В.* Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. № 4. С. 24—31.
8. *Молдовян Д. Н.* Протокол бесключевого шифрования на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 3. С. 26—32.
9. *Moldovyan D. N.* A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. № 2. P. 293—308.
10. *Moldovya N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.
11. *Горячев А. А.* Метод повышения производительности криптосхем, основанных на конечных некоммутативных группах: автореф. дисс. … канд. техн. наук по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность. — СПб, 2013. — 19 с.
12. *Молдовян Д. Н., Куприянов А. И., Костина А. А., Захаров Д. В.* Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи // Вопросы защиты информации. 2009. № 4. С. 2—7.
13. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.
14. *Moldovyan A. A.* General Method for Defining Finite Non-commutative Associative Algebras of Dimension $m > 1$ // Bulletin of Academy of Sciences of Moldova. Mathematics. 2018. № 2(87). P. 95—100.

Methods for setting non-commutative algebras as carriers of post-quantum cryptoschemes

R. Sh. Fahrutdinov, A. Yu. Mirin, I. K. Abrosimov
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS),
Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russia

In framework of the development of generalized methods for setting finite non-commutative associative algebras of different dimensions for use as algebraic carriers of post-quantum public-key cryptosystems based on the hidden discrete logarithm problem, a new unified method for setting algebras of this type is proposed and the application of the previously known embedding method for constructing four-dimensional and eight-dimensional algebras is considered. It is shown that the embedding method makes it possible to obtain eight-dimensional algebras with the vector multiplication operation, which has a lower computational complexity, while the new method has advantages when setting four-dimensional algebras.

Keywords: post-quantum cryptography, finite non-commutative algebras, finite associative algebras, local units.

Bibliography 14 references. *Received November 23, 2020*

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.772

Проблемы безопасности протокола TLS

А. О. Неволин, канд. техн. наук
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Рассмотрены принципы работы протокола TLS на примере установления соединения ("рукопожатия"). Описаны потенциальные уязвимости протокола при использовании их совместно с HTTP, связанные с возможностью анализа времени передачи пакетов и их размера. Показаны конкретные атаки CRIME и TIME. Предложены способы защиты от эксплуатации данных уязвимостей.

Ключевые слова: информационная безопасность, шифрование, TLS, HTTP, человек посередине, уязвимости протоколов.

Протокол TLS (Transport Layer Security) является криптографическим протоколом, используемым для защищенной передачи данных. Предшественником TLS является SSL (Secure Socket Layer).

TLS работает на транспортном уровне семиуровневой модели OSI и может применяться совместно с любыми широко используемыми прикладными протоколами (https для доступа к вебсайтам, POP3 / IMAP / SMTP для работы с электронной почтой и т. д.).

Протокол TLS использует следующие основные криптографические инструменты:

- асимметричное шифрование для аутентификации и обмена ключами;
- симметричное шифрование для непосредственного обмена данными;
- имитовставки с использованием секретного ключа для обеспечения целостности сообщений.

Несмотря на то что указанный протокол разработан в целях обеспечения конфиденциальности передаваемой информации, в некоторых случаях данные могут быть скомпрометированы. Рассмотрим этот вопрос более подробно.

Основные принципы работы TLS

Установление защищенного соединения (так называемое "рукопожатие") показано на рисунке.

Неволин Александр Олегович, доцент кафедры "Радиосистемы и комплексы управления, передачи информации и информационная безопасность".
E-mail: nevolin.ao@yandex.ru

Статья поступила в редакцию 26 сентября 2020 г.

Начало обмена инициирует клиент, который отправляет "приветствие" серверу. Данное сообщение содержит текущее время клиента (в формате Unix-time), случайное число и список поддерживаемых клиентов алгоритмов шифрования (в рамках допустимых в TLS).

Сервер выбирает алгоритм шифрования из предложенных, а далее в ответ отправляет свое "приветствие" с аналогичным набором данных: текущим временем, своим случайным числом и указанием на выбранный способ шифрования.

Вторым пакетом сервер отправляет клиенту свой сертификат и сообщение о завершении приветствия.

Если сертификат сервера признан корректным, клиент генерирует случайный pre-master-ключ и зашифровывает его открытым ключом сервера, который он извлек из сертификата. Для этого используют криптоалгоритм, выбранный сервером. Далее зашифрованный ключ передается на сервер.

Следующим шагом является отправка клиентом сообщения "Change cipher spec", после чего стороны прекращают обмен данными в открытом виде и переходят на шифрование трафика.

Далее обе стороны параллельно вычисляют master-ключ. Для вычисления такого ключа используют переданные ранее друг другу случайные числа и pre-master-ключ. Из master-ключа и случайных чисел сервер и клиент вычисляют ключи для симметричного шифрования, которое будет использовано для защиты всего последующего трафика.

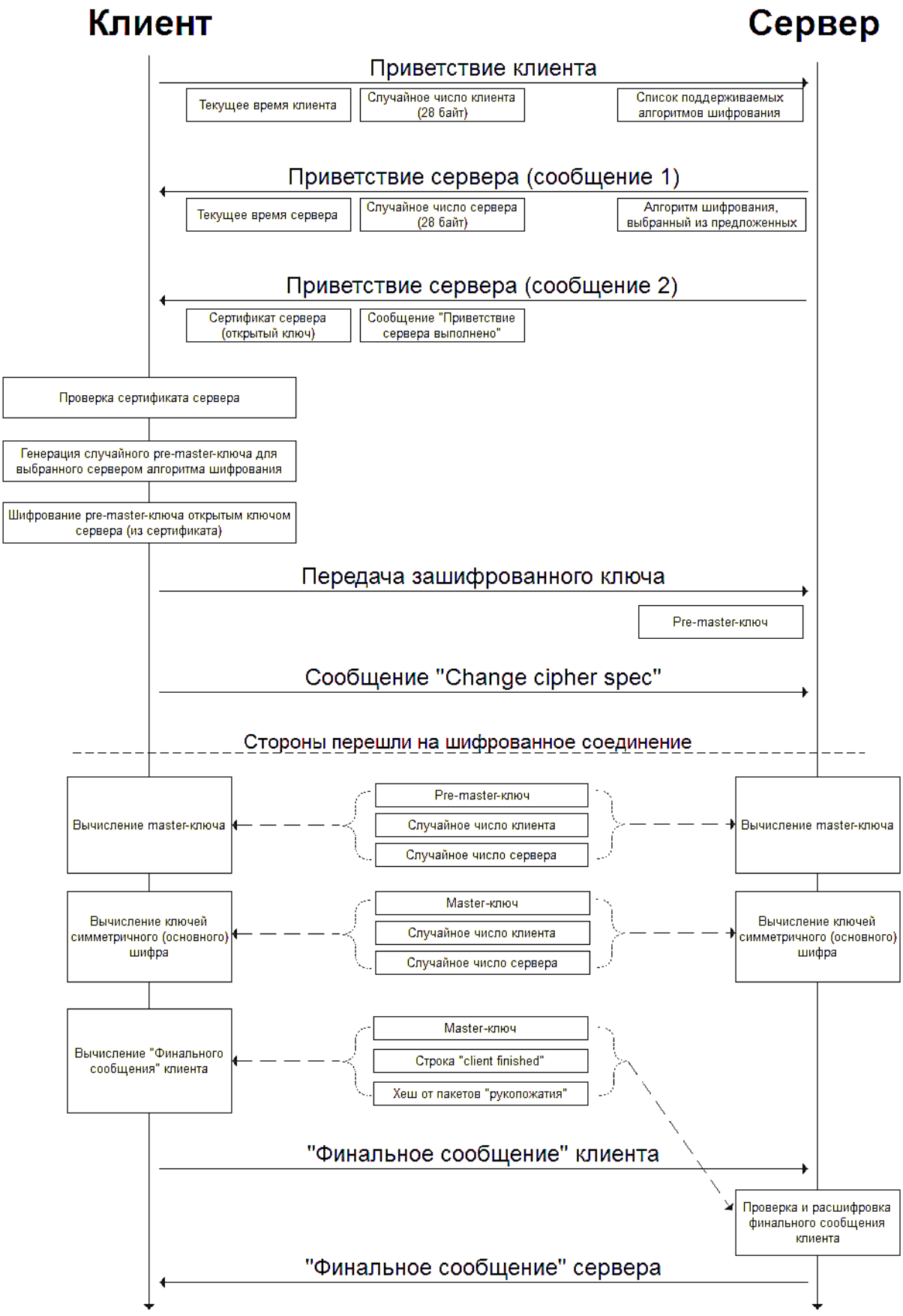

Схема установления TLS-соединения

Последним шагом является вычисление и отправка клиентом "финального сообщения". В него входят:

- master-ключ;
- текстовая строка "client finished";
- хеш от всех предыдущих сообщений "рукопожатия".

Сервер, получив такое сообщение от клиента, проверяет его корректность, а затем делает практически то же самое: отправляет клиенту сообщение с хешем от всех предыдущих сообщений и "финальное сообщение" клиента в расшифрованном виде. Таким образом, клиент может убедиться в том, что сервер смог расшифровать его сообщение.

На этом процедура установления защищенного соединения завершается, стороны начинают информационный обмен по прикладному протоколу. Все данные такого обмена шифруют симметричным шифром с помощью ключей, сгенерированных во время инициирования соединения.

Атака CRIME

Атака Compression Ratio Info-leak Made Easy (CRIME) использует некоторые механизмы сжатия, доступные в TLS, а именно DEFLATE и gzip [1].

DEFLATE по факту использует два алгоритма:

- LZ77 [1] для устранения повторяющихся последовательностей символов (слов);
- кодирование Хаффмана для сжатия идущих подряд одинаковых символов.

Алгоритм LZ77 работает по методу "сканирующего окна". Обнаружив повторяющиеся последовательности, он оставляет только одну из них, а остальные исключает, заменив на ссылку. Поиск идет в пределах окна, размер которого ограничен 32 килобайтами. Максимальный размер сравниваемой последовательности 258 байт.

Атака CRIME использует данную особенность протокола для подбора значения искомой строки (назовем ее далее секретной). Злоумышленник добавляет в заголовок HTTP-запроса угадываемую последовательность и анализирует длину пакета после сжатия. Если хотя бы 1 символ совпал, то длина последовательности уменьшится из-за применения сжатия. Этот факт будет обнаружен атакующим, поскольку он в состоянии наблюдать длину пакета независимо от применения шифрования.

Рассмотрим данную атаку подробнее на примере. Предположим, что пользователь посещает вебсайт somesite.ru. При этом клиент (браузер) отправляет на сервер HTTP-запрос:

POST / HTTP/1.1
Host: somesite.ru
User-Agent: Mozilla/6.0 (Windows NT 8) / Gecko/20150101
Cookie: secretpassword=13ab48f2c9a
Accept-Language: ru-RU,ru;
(…остальная часть запроса…)

Предполагается, что атакующий знает структуру HTTP-запроса к данному конкретному вебсайту, поскольку он может обратиться к нему самостоятельно и проанализировать отправленный заголовок.

Допустим, что злоумышленника интересует содержимое переменной cookie [2] secretpassword, т. к. в ней хранится информация о пароле пользователя, сохраненном в локальном хранилище браузера. Поскольку атакующий анализировал структуру заголовков данного сайта, он знает название соответствующей переменной и ее местоположение. Таким образом, он заранее владеет информацией о присутствии в заголовке запроса строки "secretpassword=". Эта строка продолжается последовательностью символов (секретной строкой), которая злоумышленнику неизвестна. Его цель — узнать значение данной секретной строки.

Атакующий модифицирует HTTP-запрос клиента, который теперь выглядит следующим образом:

POST /<u>secretpassword=0</u> HTTP/1.1
Host: somesite.ru
User-Agent: Mozilla/6.0 (Windows NT 8) / Gecko/20150101
Cookie: secretpassword=13ab48f2c9a
Accept-Language: ru-RU,ru;
(…остальная часть запроса…)

Подчеркиванием выделена вставка, добавленная в запрос. Как можно заметить, запрос модифицирован таким образом, чтобы строка "secretpassword=" повторилась два раза. Благодаря использованию сжатия длина зашифрованного пакета оказывается меньше приблизительно на длину этой строки N.

Далее злоумышленник формирует новый запрос, заменив добавляемую строку с "secretpassword=0" на "secretpassword=1". Теперь в запросе совпадает не строка "secretpassword=", как в предыдущем случае, а "secretpassword=1", поскольку атакующий угадал первый символ секретной строки. Вследствие этого итоговая длина пакета уменьшается уже не на N, а на $N + 1$. Хотя

злоумышленник не видит содержимого пакета, он сможет обнаружить, что длина сжатого пакета уменьшилась на 1 байт. Таким образом, атакующий поймет, что он угадал первый символ секретной строки.

Следующий шаг — аналогичный перебор 2-го символа. В тот момент, когда атакующий угадает его, длина пакета уменьшится уже на $N + 2$.

Продолжая такой перебор, злоумышленник может полностью определить значение интересующей его строки (которое может являться паролем пользователя, токеном авторизации и т. д.).

При этом атакующий может столкнуться с проблемой максимальной длины TLS-записи, которая ограничена 16 килобайтами. В случае, если пакет превышает данное значение, его разбивают на два, каждый из которых сжимается отдельно. Однако злоумышленник знает расположение секретной строки и может определить, находится ли она на границе TLS-записей. Если это так, то при вставке необходимо добавить искусственные отступы таким образом, чтобы искомая строка попала целиком в следующий пакет:

POST
/ОТСТУП_ОТСТУП_ОТСТУПsecretpassword=0
HTTP/1.1
Host: somesite.ru
User-Agent: Mozilla/6.0 (Windows NT 8) / Gecko/20150101
Cookie: secretpassword=13ab48f2c9a
Accept-Language: ru-RU,ru;
(…остальная часть запроса…)

На практике реализация данной атаки не всегда возможна, поскольку для нее должны выполняться следующие условия:

- атакующий должен иметь возможность прослушивать сетевой трафик жертвы ("человек посередине" [3]);
- жертва должна использовать вариант TLS с сжатием данных;
- в код HTML-страницы, загружаемой пользователем, должен быть внедрен специальный Javascript-код. Данный код выполняется на стороне клиента и модифицирует запросы указанным ранее способом. Для этого злоумышленнику необходимо либо разместить данный код на сайте (что не всегда возможно), либо внедрить его в трафик пользователя (например, с использованием уязвимости тега <img> [4]).

Мерой защиты от данной атаки могут быть либо отказ от TLS-сжатия (именно такая мера используется в веб-браузерах Chrome и Firefox), либо тщательный контроль за отсутствием уязвимостей веб-сайта, позволяющих внедрить чужеродный Javascript-код в тело его страниц.

Атака TIME

Атака TIME (Timing Info-leak Made Easy; "Информация о таймингах делает все простым") использует навязывание определенного содержимого в HTTP-ответах.

Данная атака в некоторой степени похожа на CRIME, однако свободна от ее недостатков:

- CRIME требует обязательного использования TLS-сжатия, которое отключено в большинстве браузеров и серверов;
- для CRIME обязательна работа атакующего по принципу "человек посередине" (Man in the Middle [3]), что не всегда возможно.

CRIME нацелена на эксплуатацию особенностей сжатия HTTP-запросов. В противовес этому TIME использует нюансы компрессии HTTP-ответов.

Рассмотрим кратко некоторые механизмы и термины информационного обмена.

SOP (Same Origin Policy) — механизм, регулирующий возможность кода Javascript, расположенного в теле страницы, получать доступ к объектам модели DOM [2] других сайтов (доменных имен). В основном такой доступ запрещен. Однако в некоторых случаях, например для мультимедийных тегов (в частности, img), доступ разрешен. Это приводит к некоторым уязвимостям, которые хорошо описаны в [4], и позволяет внедрить вредоносный Javascript-код.

MTU (Maximum Transmission Unit) — максимальный размер пакета IP, который может быть передан единым целым. Как правило, он варьируется в пределах от 128 байт до 10 килобайт. Типовое значение в сети Интернет 1500 байт. Если размер пакета превышает значение MTU, то он фрагментируется (разбивается на несколько частей).

RTT (Round Trip Time) — время, затрачиваемое на отправку IP-пакета и получение подтверждения от адресата.

MSS (Maximum Segment Size) — максимальный объем полезных данных, который может быть передан в нефрагментированном IP-пакете. Как правило, он равен значению MTU за вычетом длины IP-заголовка и TCP-заголовка:

MSS = MTU — [длина заголовка TCP] — [длина заголовка IP].

TCP Sliding Window System — механизм, предназначенный для оптимизации передачи данных.

Он позволяет отправителю передать все необходимые пакеты и только после этого получить подтверждение от адресата (пакет ACK).

Общая идея атаки TIME заключается в искусственном увеличении длины HTTP-ответа таким образом, чтобы произошла фрагментация и он был разбит на два пакета. RTT одного и двух пакетов значительно отличаются и могут быть объектом анализа.

Предположим, что:

- В HTTP-ответе присутствует какой-нибудь секретный параметр, интересующий атакующего (например, токен авторизации);
- Веб-страница устроена таким образом, что пользователь может вводить некоторые значения, которые будут присутствовать в HTTP-ответе (например, пользователь вводит свой логин, а затем возвращается к HTML-разметке для отображения строки "Вы вошли как…"). Назовем данный принцип зеркалированием пользовательского ввода.

Злоумышленник внедряет на HTML-страницу вредоносный Javascript-код (скрипт), который будет отсылать запросы на сервер. В таких запросах скрипт имитирует ввод пользователем значения (логин из приведенного примера). При этом используют следующие принципы.

- Сначала скрипт подбирает такую длину пользовательского параметра, при которой происходит разбиение одного пакета на два (факт разбиения сравнительно легко обнаружить, анализируя RTT).
- После этого скрипт пытается "угадать" первую букву секретного параметра, добавляя ее к пользовательскому вводу. Если буква угадана неверно, то пакет будет разбит на два. Если буква угадана верно, то произойдет сжатие HTTP-ответа (поскольку она присутствует и в зеркалированном пользовательском параметре, и в секретном). Его длина сократится, и пакет не будет разделен. Данный факт будет также определен путем анализа RTT.
- Угадав первую букву, скрипт добавляет 1 символ смещения и пытается угадать вторую и т. д. до угадывания всей секретной последовательности.

Для успешного выполнения данной атаки злоумышленник должен знать название секретного параметра, его местоположение, а также быть уверенным в наличии зеркалирования пользовательского ввода. Однако поскольку атакующий сам может обращаться к сайту, выявление такой информации не составляет проблемы.

Также осуществлению атаки могут препятствовать так называемые шумы сети — явления, вызывающие изменение RTT (например, маршрутизация или потеря пакетов). Однако путем анализа RTT нескольких одинаковых пакетов злоумышленник может найти среднее или минимальное значение и далее опираться на него.

В качестве мер противодействия данной атаке можно использовать:

- добавление случайной задержки при передаче HTTP-ответа (что сделает невозможным достоверное вычисление RTT на стороне атакующего);
- отказ от зеркалирования пользовательского ввода на веб-странице;
- привлечение механизмов, предотвращающих автоматизацию запросов к сайту (CAPTCHA и другие).

Заключение

Протокол TLS изначально был разработан для защиты передаваемых данных путем их шифрования. В ходе своего развития он претерпел множественные изменения, призванные улучшить его производительность и защищенность.

Несмотря на это, версии протокола имеют ряд уязвимостей. Данные уязвимости являются, скорее, косвенными, т. е. могут быть использованы лишь при ряде условий и ограничений. Тем не менее реальная практика показывает, что такие условия достижимы.

Описана схема работы протокола TLS и указаны некоторые его проблемы, которые могут косвенно приводить к компрометации передаваемых данных.

Приведены меры защиты от эксплуатации таких уязвимостей.

Литература

1. *Ватолин Д., Ратушняк А., Смирнов М., Юкин В.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. — М.: Диалог-МИФИ, 2003. — 384 с.

2. *Кришнамурти Б., Рексфорд Д.* Web-протоколы. Теория и практика. — М.: Бином, 2010. — 592 с.

3. О некоторых приемах атаки Man in the middle [Электронный ресурс]. — Режим доступа: https://habr.com/ru/post/131710/

4. Script in IMG tags [Электронный ресурс]. — Режим доступа: https://www.owasp.org/index.php/Script_in_IMG_tags

TLS security issues

A. O. Nevolin
Moscow Aviation Institute (National Research University), Moscow, Russia

Article describes TLS protocol principles by example of connection establishment (handshake). Potential vulnerabilities by using HTTP protocol are described. These vulnerabilities are based on packet timings and size analysis. Example of CRIME and TIME attacks are shown. Different counter-measurements are described.

Keywords: information security, encryption, TLS, HTTP, man-in-the-middle, protocol vulnerabilities.

Bibliography — 4 references. *Received September 26, 2020*

УДК 004.056.5+004.712

Однонаправленная передача данных между компьютерными сетями с различными категориями обрабатываемой информации

С. П. Панасенко, канд. техн. наук
ООО Фирма «АНКАД», Москва, Россия

Рассмотрена проблема обеспечения строго однонаправленной передачи данных при взаимодействии между вычислительными сетями, обрабатывающими информацию различных уровней конфиденциальности. Описано решение данной проблемы на основе применения специализированных сетевых адаптеров с одиночным оптическим сетевым интерфейсом.

Ключевые слова: однонаправленная передача данных, предотвращение утечки данных, локальная вычислительная сеть, волоконно-оптическая связь.

Проблема передачи данных между разнокатегорийными вычислительными сетями

В распределенных информационных системах в ряде случаев возникает задача безопасной передачи данных между локальными вычислительными сетями (ЛВС), в которых обрабатывают информацию различных категорий (с точки зрения требований по обеспечению конфиденциальности обрабатываемой информации). В числе прочего безопасность передачи данных в данном случае подразумевает одновременное обеспечение следующих двух условий:

- возможности передачи данных из сети менее строгой в сеть более строгой категории;
- отсутствия даже теоретической возможности передачи информации из сети более строгой в сеть менее строгой категории.

Указанные условия фактически являются требованием обеспечения строгой однонаправленности передачи данных, когда во избежание утечки информации никакие информационные сигналы не могут физически передаваться из сети более строгой в сеть менее строгой категории.

Первое из приведенных условий легко выполнимо, тогда как второе при использовании традиционных способов передачи данных между ЛВС является практически невыполнимым. Поэтому наиболее распространенным способом обеспечения однонаправленности передачи данных из сети менее строгой в сеть более строгой категории является следующий (см. рис. 1):

- разнокатегорийные сети разделяют физически, т. е. обеспечивается отсутствие средств вычислительной техники и сетевого оборудования, подключенных к двум разнокатегорийным сетям одновременно;
- передачу данных осуществляют путем их переноса на каком-либо отчуждаемом носителе.

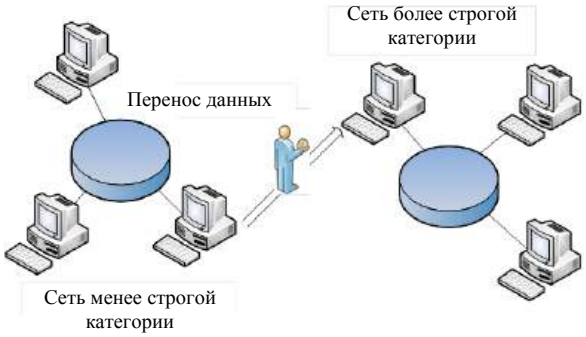

Рис. 1. Традиционная однонаправленная передача данных

Носитель для переноса данных также должен отвечать дополнительным требованиям, обеспечивающим невозможность утечки данных из сети более строгой в сеть менее строгой категории, включая следующие:

- он не должен быть перезаписываемым, т. е. должен допускать строго однократную запись;
- с возможностью многократной записи может использоваться только однократно или в том случае, когда рабочее место сети более строгой категории (к которому физически подключается носитель) оснащается надежным средством блокировки записи на носители используемого типа.

Описанный способ обладает крайне низкими эксплуатационными характеристиками. При этом основным его недостатком можно считать невозможность передачи информации в режиме реаль-

Панасенко Сергей Петрович, заместитель директора по науке и системной интеграции.
E-mail: sp@ancud.ru

Статья поступила в редакцию 1 декабря 2020 г.

ного времени, т. е. невозможность обеспечения сети более строгой категории поступающей в сеть менее строгой категории актуальной информацией в момент ее поступления. Таким образом, задача физического соединения разнокатегорийных сетей с обеспечением однонаправленной передачи данных является актуальной.

Использование однонаправленного оптического канала связи для передачи данных

При еще относительно недавно повсеместно используемых проводных технологиях передачи данных задача выглядела нерешаемой, поскольку при наличии физического медного кабеля, соединяющего две ЛВС, невозможно обеспечить доказуемое отсутствие утечки данных по такому кабелю в обратном направлении. Аналогично невозможно обеспечить однонаправленную передачу данных с помощью беспроводных технологий, применяемых для построения вычислительных сетей.

С появлением оптоволоконных линий передачи данных обеспечение строго однонаправленной передачи данных из сети менее строгой в сеть более строгой категории стало возможным.

Волоконно-оптическая связь использует для передачи информации электромагнитное излучение оптического диапазона в качестве носителя информационного сигнала. Волоконно-оптический кабель содержит световод, который является направляющим для излучаемых электромагнитных волн. При этом подключение кабеля с одной стороны к передатчику и с другой — к приемнику обеспечивает однонаправленную передачу данных в одном кабеле. Для сетевых подключений используют пару кабелей, каждый из которых обеспечивает передачу данных в одном направлении [1].

Таким образом, решить проблему строго однонаправленной передачи данных можно с помощью пары специальных сетевых адаптеров, один из которых имеет только передающую часть оптического сетевого интерфейса, а другой — только приемную. Данные сетевые адаптеры подключают следующим образом:

- передающий сетевой адаптер устанавливают на компьютер, расположенный в ЛВС с менее строгой категорией обрабатываемых данных (в качестве примера такой ЛВС можно привести ЛВС, в которой не обрабатывается конфиденциальная информация и имеется подключение к сети Интернет) и предназначенный для передачи данных в ЛВС с более строгой категорией;
- принимающий сетевой адаптер устанавливают на компьютер, расположенный в ЛВС с более строгой категорией (в качестве примера приведем ЛВС, в которой обрабатывается информация, предназначенная для служебного пользования) и предназначенный для приема данных из ЛВС с менее строгой категорией;
- к указанным сетевым адаптерам подключают одиночный волоконно-оптический кабель, обеспечивающий передачу данных только от сетевого адаптера с передающей частью оптического сетевого интерфейса к сетевому адаптеру с приемной частью оптического сетевого интерфейса.

Таким образом, специальные сетевые адаптеры с одиночным сетевым интерфейсом позволяют обеспечить передачу данных строго в одну сторону: от передающего сетевого адаптера к приемному, т. е. из ЛВС с менее строгой в ЛВС с более строгой категорией обрабатываемых данных. Обратный сетевой интерфейс физически отсутствует, что при отсутствии альтернативных подключений между этими вычислительными сетями обеспечивает строго однонаправленную передачу данных.

Общая схема подобной системы, осуществляющей однонаправленную передачу данных, приведена на рис. 2.

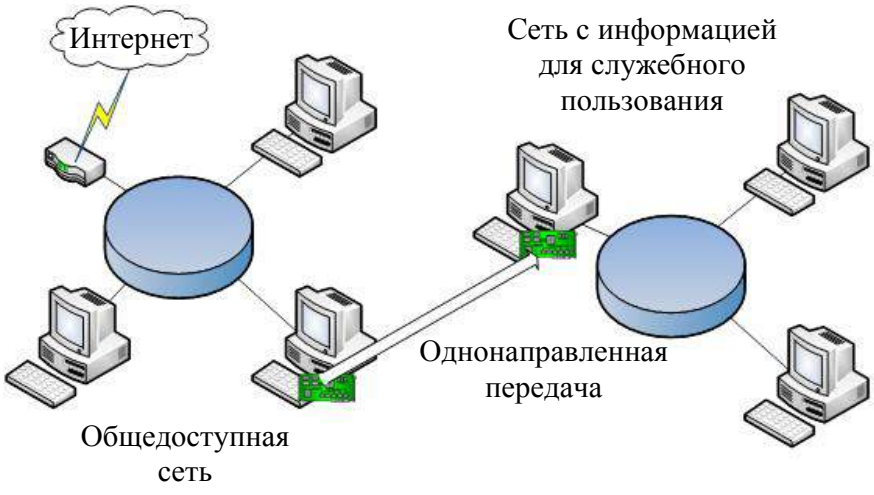

Рис. 2. Однонаправленная передача данных с помощью сетевых адаптеров с одиночным сетевым интерфейсом

На рис. 3 приведен пример подобного специализированного сетевого адаптера, оснащенного только приемным оптическим сетевым интерфейсом.

Рис. 3. Сетевой адаптера с одиночным оптическим интерфейсом

Несмотря на кажущуюся простоту данного решения, необходимо отметить, что при его реализации существует ряд технических проблем, основной из которых является необходимость в наличии обратной связи, предусмотренная в ряде сетевых протоколов передачи данных. Примером такой обратной связи служит подтверждение получения данных, обязательное в ряде сетевых протоколов.

В частности, широко используемый протокол транспортного уровня TCP (Transmission Control Protocol) [2] требует, во-первых, активных действий второй стороны обмена данными при установлении соединения, а во-вторых, подтверждений принятых данных для обеспечения гарантированной доставки, установления оптимальной скорости обмена данными и прочих целей.

При физическом отсутствии обратного сетевого соединения обеспечить реальную обратную связь невозможно. Поэтому приходится отказаться от использования TCP и подобных ему протоколов, требующих информативной обратной связи, в однонаправленном сетевом соединении. Это касается, в частности, и протоколов защищенной передачи данных, например TLS (Transport Layer Security) [3] или IPSec (Security Architecture for the Internet Protocol) [4], также предусматривающих активное участие обеих сторон информационного обмена.

Указанные проблемы могут быть решены следующим образом:

- на транспортном уровне используют протокол UDP (User Datagram Protocol) [5], не требующий установки соединений и каких-либо подтверждений; при этом данные передаются со значительной избыточностью, искусственно вносимыми временны́ми задержками и контролем целостности (например, на основе применения алгоритмов хэширования); совокупности этих мер достаточно для обеспечения однонаправленной передачи данных с контролем их возможных искажений на принимающей стороне;
- при необходимости защищенной передачи данных (в зашифрованном виде) их шифрование может быть организовано на файловом уровне средствами, установленными в операционной системе компьютеров, оснащенных специализированными сетевыми адаптерами.

При наличии в распределенной информационной системе вычислительных сетей нескольких различных категорий подобные специализированные сетевые адаптеры можно использовать каскадно для многоступенчатой передачи данных.

Заключение

Проблема обеспечения строго однонаправленной передачи данных из ЛВС менее строгой категории в ЛВС более строгой категории может быть решена за счет использования специализированных сетевых адаптеров, оснащенных только передающей или только приемной частью оптического сетевого интерфейса, в совокупности с программным обеспечением, позволяющим организовать однонаправленную передачу данных с контролем их целостности на принимающей стороне.

Литература

1. Волоконно-оптическая связь [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Волоконно-оптическая_связь
2. RFC 793. Transmission Control Protocol. DARPA Internet Program. Protocol Specification [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc793
3. *Dierks T., Rescorla E.* RFC 5246. The Transport Layer Security (TLS) Protocol. Version 1.2 [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc5246
4. *Kent S., Seo K.* RFC 4301. Security Architecture for the Internet Protocol [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc4301
5. *Postel J.* RFC 768. User Datagram Protocol [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc768

Unidirectional data transfer between computer networks with different categories of processed information

S. P. Panasenko
ANCUD Ltd., Moscow, Russia

The article considers the problem of strictly unidirectional data transmission providing between computer networks that process information of different confidentiality levels. It describes a solution of this problem based on the use of special network adapters with an unidirectional optical network interface that can transmit or receive only.

Keywords: unidirectional data transmission, data leakage prevention, local area network, fiber-optic communication.

Bibliography — 5 references. *Received December 1, 2020*

ДОВЕРЕННАЯ СРЕДА

УДК 004.932

Применение сверточных нейронных сетей для стилизации изображений

А. В. Силин, канд. техн. наук; *И. В. Силина*; *О. Н. Гринюк*, канд. техн. наук
Новомосковский институт (филиал) Российского химико-технологического университета им. Д. И. Менделеева, г. Новомосковск, Тульская обл., Россия

О. В. Алексашина, канд. техн. наук
Московский политехнический университет, Москва, Россия

Л. Н. Паршина, канд. эконом. наук
ФГБОУ ВО "Петербургский государственный университет путей сообщения Императора Александра I", Санкт-Петербург, Россия

Представлены методы применения сверточных нейронных сетей для переноса стиля одного изображения на другое. Сделан вывод, согласно которому один метод превосходит другой. Выполнена оценка их ресурсоемкости и эффективности.

Ключевые слова: сверточная нейронная сеть, глубокое обучение, стилизация, распознавание объектов.

Нейронная сеть представляет собой математическую модель с последующим воплощением в виде аппаратной или программной реализации, базирующуюся на биологических нейронных сетях. Нейронные сети применяют в различных сферах деятельности. Рассмотрим те из них, которые работают с графической информацией.

Последние несколько лет набирают популярность различного рода методы модификации фотографий. В отличие от типичных преобразований (размытие, искажение, выделение каких-либо деталей, контраст и т. п.) преобразования с помощью нейронных сетей открывают более широкий круг возможностей. Одним из подобных направлений является перенос стиля одних изображений, таких, как картины или иллюстрации, на другие.

Силин Андрей Владимирович, доцент, заведующий кафедрой.
E-mail: asilin@nirhtu.ru
Силина Ирина Викторовна, старший преподаватель.
E-mail: isilina@nirhtu.ru
Гринюк Ольга Николаевна, доцент.
E-mail: olgrinyuk@mail.ru
Алексашина Ольга Вячеславовна, доцент.
E-mail: Svirukova@yandex.ru
Паршина Любовь Николаевна, доцент.
E-mail: parshinaln@yandex.ru

Статья поступила в редакцию 17 ноября 2020 г.

Решение задачи наложения стиля, позволяющего сделать из фотографии картины, которая была поставлена и решена L. Gatys [1] в 2016 г., требует использования более сложного метода, которым в итоге стали сверточные нейросети. Сверточные сети способны находить на изображениях отдельные объекты или значимые части объектов, также называемые высокоуровневыми признаками (пиксели изображения можно считать низкоуровневыми признаками). Эта их способность позволяет эффективно различать объекты на изображении, восстанавливать некоторые величины, например расстояние до объектов, и модернизировать изображения с сохранением высокоуровневых признаков. На последнем принципе и основан нейронный перенос стиля.

Существует несколько подходов к стилизации изображений. Рассмотрим два подхода.

Первый из них был предложен Leon A. Gatys в 2016 г. В его работе перенос стиля с одного изображения на другое может быть рассмотрен как задача переноса текстуры. При передаче текстуры цель состоит в том, чтобы синтезировать текстуру из исходного изображения, в то же время сдерживая синтез текстур для того, чтобы сохранить семантическое содержание целевого изображения.

Задача решается при помощи нейронной сети VGG (Visual Geometry Group) — предобученной на большом наборе изображений imagenet-нейросети, которая решает задачу поиска объек-

тов. Данная модель предложена K. Simonyan и A. Zisserman в [2]. При тестировании на ImageNet и наборе данных из порядка 15 млн размеченных категорированных изображений достигается высокая точность в задаче распознавания объектов на изображении (рис. 1).

Функция потери контента показывает, насколько похожи исходное изображение X и сгенерированное изображение Y, но не сравнивает их попиксельно, а находит похожие высокоуровневые признаки и сравнивает их. Функция имеет вид

$$L^l_{\text{con}}(X, Y_{\text{con}}) = \frac{1}{HWC}\sum_{c=1}^{c}\sum_{i=1}^{h}\sum_{j=1}^{w}\left(X^l_{ijc} - Y^l_{ijc}\right)^2, \qquad (1)$$

где X^1, Y^1 — карты признаков, полученные после применения нейросети к изображениям X и Y в l-м слое нейросети;

H, W, C — их размеры и число каналов соответственно.

Для визуализации информации изображения, которая закодирована на разных уровнях иерархии, можно применить оптимизацию методом градиентного спуска на изображении белого шума, чтобы найти другое изображение, которое соответствует характеристическим откликам исходного.

Для нахождения близости по стилю используют матрицу Грама, вычисляемую по формуле

$$G_l(X) = \frac{1}{H_l W_l} F_l(x)^{\mathrm{T}} F_l(x) \in \mathbf{R}^{C_l \times C_l}. \qquad (2)$$

Если интерпретировать $F_1(x)$ как матрицу, состоящую из объектов размерности C_1, то матрица Грама будет равна нецентрированной матрице ковариаций. Таким образом, матрица Грама содержит информацию о том, какие каналы карты признаков зависят друг от друга. Тогда функция потерь, отвечающая за перенос стиля X_{st}, определяется по формуле

$$L^l_{\text{st}}(X, Y_{\text{st}}) = \frac{1}{C_l^2}\left\|G_l(Y_{\text{st}}) - G_l(X)\right\|^2_F. \qquad (3)$$

Чтобы перенести стиль картины a на фотографию p, синтезируют новое изображение, которое одновременно соответствует представлению содержимого p и представлению стиля a. Таким образом, минимизируется разница между будущим изображением, получаемым из белого шума на основе фотографии в одном слое, и стилем картины, определенной на нескольких слоях сверточной нейронной сети. Функция потерь имеет вид

$$L_{\text{tod}}(X, Y_{\text{con}}, Y_{\text{st}}) = \\ = \sum \beta^l_{\text{con}} L^l_{\text{con}}(Y_{\text{con}}, X) + \alpha \sum \beta^l_{\text{st}} L^l_{\text{st}}(Y_{\text{st}}, X). \qquad (4)$$

Другой подход к стилизации изображений, описанный Depth-aware Neural Style Transfer [3], имеет схожие черты с описанным методом, однако здесь предложено оптимизировать не изображение, полученное из белого шума, а результат работы нейронной сети, которая подготавливает стилизуемое изображение. В качестве такой сети используют сеть с чередующимися и дробно расположенными свертками. Она содержит два слоя понижения разрешения (*downsampling*) и два слоя увеличения разрешения (*upsampling*). Предполагается, что после всех преобразований будет возможно использовать бóльшие сети при тех же вычислительных затратах, что и без этого вспомогательного преобразования. Для сохранения особенностей исходного изображения также вводят дополнительную сеть оценки глубины (рис. 2).

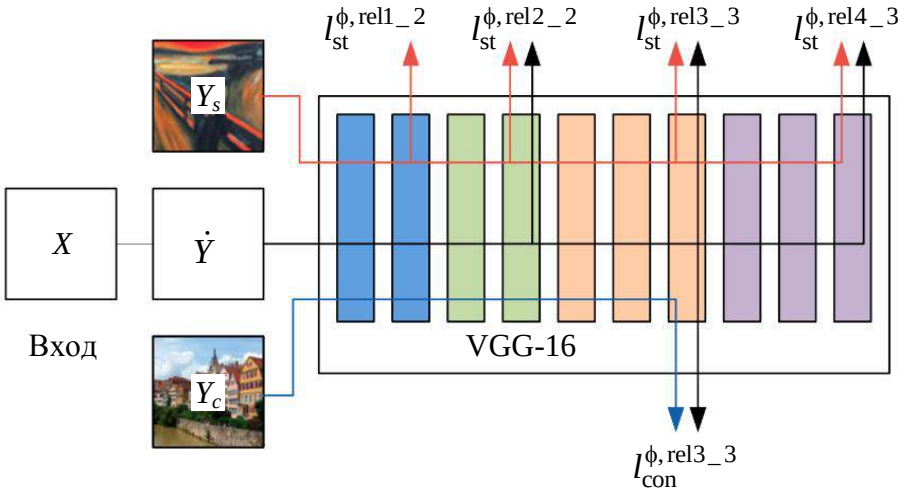

Рис. 1. Схема тестирования на нейронной сети VGG

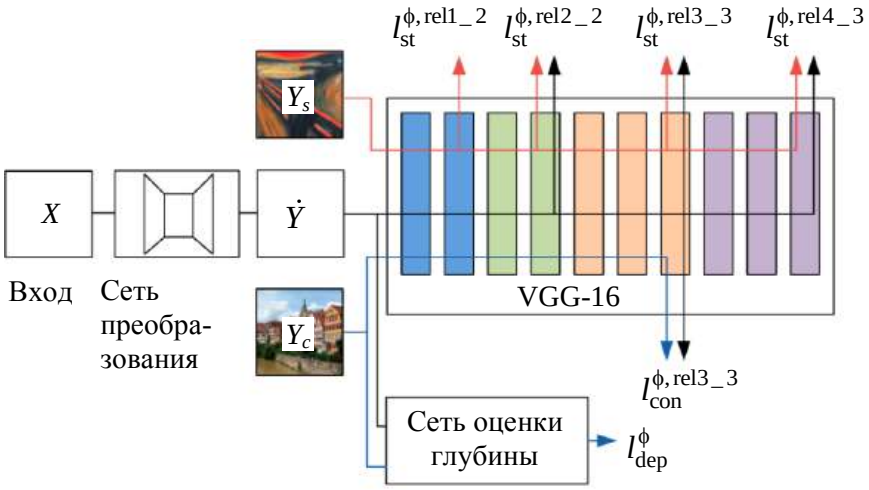

Рис. 2. Схема тестирования нейронной сети на основе стилизации изображения

Функцию потери глубины используют для оценки разности между преобразуемым изображением и целевым изображением. Для максимального сохранения информации о глубине и структурных особенностях применяют соответствующую сеть. Данные с её выхода используют для вычисления дистанций. Указанная функция имеет вид

$$l_{dep}^{\phi 1}\left(X, Y_{con}\right)=\frac{1}{HWC}\left\|\phi_1\left(Y_{con}\right)-\phi_1\left(X\right)\right\|_2^2. \qquad (5)$$

Итоговая функция потерь не сильно отличается от предыдущего варианта:

$$L_{tot}\left(X, Y_{con}, Y_{st}\right)=\sum\beta_{con}^{l}L_{con}^{l}\left(Y_{con}, X\right)+ \\ +\alpha\sum\beta_{st}^{l}L_{st}^{l}\left(Y_{st}, X\right)+\delta\sum\beta_{dep}^{l}L_{dep}^{l}\left(Y_{dep}, X\right). \qquad (6)$$

При синтезе изображения, оптимизирующего потери стиля, контента и глубины, невозможно добиться одновременно полного соответствия всем этим критериям. Однако поскольку итоговая функция потерь является линейной комбинацией её составляющих, существует возможность устанавливать весовые коэффициенты этих факторов. Например, делая упор на стиль, можно потерять общий макет изображения. На рис. 3 наглядно сравниваются эти два метода.

а

б *в*

Рис. 3. Наглядное сравнение:
а — исходное изображение; *б* — обычная стилизация; *в* — стилизация с учетом глубины

Таким образом, для исследования была применена математическая библиотека Torch с использованием фреймворка для глубокого обучения Caffe. В качестве сети распознавания объектов применена сеть VGG-16. Для оптимизации использован алгоритм Adam.

В результате проведенного исследования выявлено, что из двух представленных методов более эффективным можно считать метод, описанный в Depth-aware Neural Style Transfer, так как в этом случае системе нет необходимости восстанавливать изображение из белого шума и подаваемое на вход изображение уже приведено к оптимальному виду посредством вспомогательной сети преобразования изображения. Полученное изображение также превосходит результат метода L. Gatys по чёткости деталей за счёт введения дополнительной сети оценки глубины.

Перечисленные методы нельзя назвать лучшими, так как они весьма требовательны к ресурсам вычислительной машины. Это также объясняется и основными недостатками самой сети VGG: низкая скорость обучения и тяжеловесность архитектуры. Большое количество полносвязных узлов и глубина делают процесс развертывания сети затруднительным. Возможно, более предпочтительными будут меньшие архитектуры (GoogLeNet, Xception, SqueezeNet и другие).

Литература

1. *Gatys L. A., Ecker A. S., Bethge M.* Image Style Transfer Using Convolutional Neural Networks: Conference on CVPR, 2016. P. 216—220
2. *Simonyan K., Zisserman A.* Very Deep Convolutional Networks for Large-Scale Image Recognition: ICLR, 2015. P. 34—42.
3. *Xiao-Chang Liu, Ming-Ming Cheng, Yu-Kun Lai, Rosin P. L.* Depth-aware Neural Style Transfer: Non-Photorealistic Animation and Rendering Conference, 2017. P. 81—88.

Application of convolutional neural networks for styling images

A. V. Silin, I. V. Silina, O. N. Grinyuk
Nomoskovsk Institute (branch) of the Russian Chemical-Technological University named after D. I. Mendeleev, Novomoskovsk, Tula region, Russia

O. V. Aleksashina
Moscow Polytechnic University, Moscow, Russia

L. N. Parshina
St. Petersburg State University of Railway Transport of Emperor Alexander I, St. Petersburg, Russia

Methods using convolutional neural networks to transfer the style of one image to another are considered. It is concluded, that one method is superior to another, the evaluation of their resource intensity and efficiency.

Keywords: convolutional neural network, deep learning, styling, object recognition.

Bibliography — 3 references. *Received November 17, 2020*

УДК 519.24; 53; 57.017

Оценка ускорения вычислений в режиме программного воспроизведения эффектов нейродинамики при извлечении знаний из больших сетей искусственных нейронов

А. И. Иванов, д-р техн. наук
АО «Пензенский научно-исследовательский электротехнический институт», г. Пенза, Россия

А. И. Газин, канд. техн. наук
ФБГОУ ВО «Липецкий педагогический университет им. П. П. Семенова-Тян-Шаньского», г. Липецк, Россия

А. Е. Сулавко, канд. техн. наук; *Д. Г. Стадников*
ФГБОУ ВО «Омский государственный технический университет», г. Омск, Россия

Рассмотрена оценка ускорения, получаемая при модуляции входных данных большой сети искусственных нейронов, выполняемой в соответствии с требованиями семи отечественных стандартов серии ГОСТ Р 52633.xx. Использована модуляция входных данных исследуемой сети искусственных нейронов скрещиванием биометрических образов-родителей и получением от них биометрических образов-потомков по ГОСТ Р 52633.2-2011.

Ключевые слова: искусственные нейроны, большие данные, модуляция входных данных, нейродинамика.

Цифровая экономика предполагает безопасность выполнения Интернет-операций между людьми и при взаимодействии людей с облачными технологиями. Идентификация пользователя при входе в локальный компьютер или при дистанционном входе через Интернет в личный кабинет выполняется через ручной ввод человеком короткого логина и короткого пароля. Проблема состоит в том, что короткие, легко запоминаемые людьми пароли легко подбираются злоумышленниками.

Эта проблема может быть решена мировым сообществом через использование биометрической идентификации и аутентификации [1, 2]. Важность решаемой задачи подтверждается тем, что в 2002 г. по этому направлению развития был создан международный технический комитет ISO/IEC JTC1 sc37 (Биометрия). С момента создания усилиями ISO/IEC JTC1 sc37 было разработано 153 международных стандарта по биометрии. Защитой биометрии занимается международный технический комитет ISO/IEC JTC1 sc27 (Защита информации и приватности). Этот комитет разработал три международных стандарта по защите биометрических данных шифрованием, однако они непригодны для применения в Интернет-приложениях.

За рубежом проблему защиты персональных биометрических данных Интернет-приложений пытаются решать путем использования так называемых нечетких экстракторов [3—5], ориентируясь на слабую криптографию коротких ключей. Ориентация зарубежных технологий на короткие ключи — вынужденная мера. Биометрические образы, как правило, позволяют извлекать сотни биометрических параметров. Например, среда моделирования БиоНейроАвтограф [6] построена на анализе динамики рукописного почерка и позволяет извлекать из биометрического образа 416 биометрических параметров. Если для анализа 416 биометрических параметров попытаться использовать "нечеткий экстрактор", получится длина ключа 416/30≈14 бит при условии использования классических кодов, обнаруживающих и исправляющих ошибки и обладающих 30-кратной избыточностью. Стойкость к подбору столь короткого ключа меньше стойкости пароля из двух случайных символов.

Иванов Александр Иванович, доцент, научный консультант.
E-mail: bio.ivan.penza@mail.ru; ivan@pniei.penza.ru
Газин Алексей Иванович, доцент.
E-mail: itizi@lspu-lipetsk.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Стадников Денис Геннадьевич, инженер-программист.
E-mail: sdg250598@inbox.ru

Статья поступила в редакцию 25 ноября 2020 г.

Проблема коротких биометрических ключей и коротких биометрических паролей решается применением искусственных нейронных сетей, выполненных по требованиям 7 отечественных национальных стандартов серии ГОСТ Р 52633.хх. Это технологическое направление предполагает наличие одного искусственного нейрона на один бит криптографического ключа. Таким образом, длина криптографического ключа зависит от числа искусственных нейронов и может быть любой. На рис. 1 приведен пример применения сети из 256 искусственных нейронов.

Очевидно, что хакер легко подберет код пароля доступа из 2 символов и не способен подобрать пароль, состоящий из 32 случайных символов. Как следствие все системы парольной аутентификации построены таким образом, чтобы скрыть длину пароля доступа от хакера. Системы биометрико-парольной аутентификации должны строиться по-другому и демонстрировать хакеру необходимость ввода при доступе длинного пароля. Пример организации соответствующего индикатора доступа приведен на рис. 2.

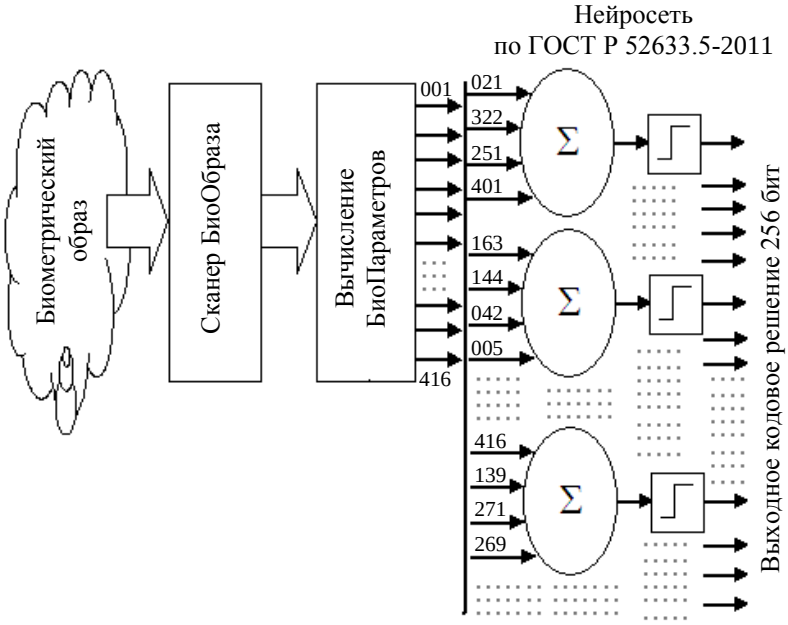

Рис. 1. Структура нейросетевого преобразователя биометрического образа человека в код его криптографического ключа (случайного пароля) длиной в 256 бит

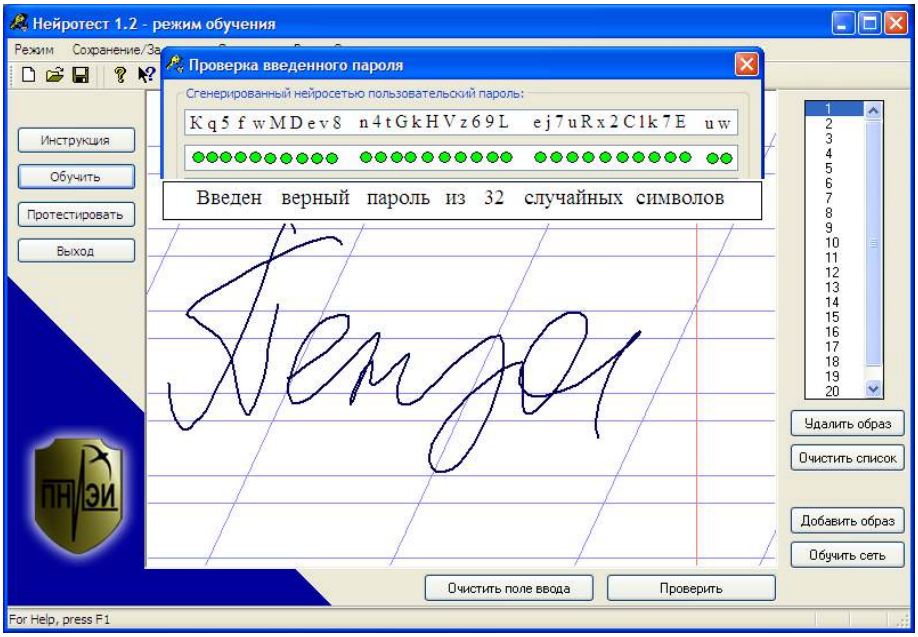

Рис. 2. Экранная форма режима обучения среды моделирования БиоНейроАвтограф на фоне индикатора доступа, подтверждающего обнаружение верного пароля доступа из 32 случайных символов

Основные требования к нейросетевым преобразователям биометрия—код

Первым требованием базового стандарта ГОСТ Р 52633.0-2006 является полностью автоматическое обучение сети искусственных нейронов алгоритмом ГОСТ Р 52633.5-2011 на малой выборке примеров биометрического образа "Свой". Пользователь не должен обладать особыми знаниями и умениями. Пользователю должно быть достаточно ввести 20 примеров образа "Свой" и инициировать процесс обучения. После обучения нейросети все примеры обучающей выборки должны быть уничтожены.

Вторым требованием является автоматическое создание программным приложением случайных паролей или ключей доступа длиной в 256 бит, которые во время обучения будут безопасно связаны с примерами образа "Свой". Допустим также экспорт криптографического ключа из внешних приложений.

Третьим требованием ГОСТ Р 52633.0-2006 является наличие встроенных в приложение средств автоматической оценки вероятности появления ошибок первого рода (P_1 — вероятность ошибочного отказа пользователю "Свой" в доступе).

Четвертым требованием является наличие встроенных в приложение средств автоматической оценки вероятности появления ошибок второго рода (P_2 — вероятность случайного принятия образа "Чужой" как образа "Свой"). Средство быстрого самотестирования должно иметь тестовую базу образов "Чужой", сформированную по ГОСТ Р 52633.1-2009. Само тестирование должно выполняться алгоритмом ГОСТ Р 52633.3-2011.

Пятым требованием базового стандарта ГОСТ Р 52633.0-2006 является равная вероятность появления состояний "0" и состояний "1" в каждом из 256 разрядов выходного кода при воздействии на обученную сеть искусственных нейронов биометрическими образами тестовой базы "Чужой".

Если выполнены перечисленные требования, то сеть искусственных нейронов практически полностью устраняет входную 416-мерную энтропию примеров образа "Свой" и/или 256-мерную энтропию кодов "Свой":

$$H(\nu_{001}, \nu_{002}, ..., \nu_{416}) \approx$$

$$\approx H("c_{001}, c_{002}, ..., c_{256}") \approx \qquad (1)$$

$$\approx -\log_2(1-P_1) \approx -\log_2\left(1-\frac{1}{20+1}\right) \approx 0,07,$$

при условии тестирования нейросети на 20 примерах образа "Свой" без обнаружения факта отказа в доступе.

Для биометрических образов "Чужой" возникает обратный эффект усиления естественной 416-мерной энтропии примеров образа и/или 256-мерной энтропии кодов, порождаемых примерами образа "Чужой":

$$H(\xi_{001}, \xi_{002}, ..., \xi_{416}) \approx$$

$$\approx H("x_{001}, x_{002}, ..., x_{256}") \approx \qquad (2)$$

$$\approx -\log_2(P_2) \approx 28,0 - 56,0.$$

Следует подчеркнуть, что хакер, не имеющий доступа к преобразователю биометрия—код, вынужден подбирать случайный пароль с 2^{256} или 8^{32} состояниями. Эта задача имеет очень высокую вычислительную сложность. Обнаружив столь надежную защиту (см. рис. 2), хакер, скорее всего, откажется от проведения атаки.

Совершенно иная ситуация возникает, когда хакеру удается похитить у пользователя нейросетевой преобразователь биометрия—код. В этом случае стойкость к атакам подбора со стороны биометрии будет сопоставима со стойкостью паролей, имеющих от 4 до 8 случайных знаков. С такой задачей хакер может справиться примерно за 10 мин, если у него есть заранее созданная база из 10 000 образов "Чужой".

Атака по извлечению знаний из обученной нейросети при незащищенном хранении ее таблиц связей и таблиц весовых коэффициентов ее нейронов

По определению, коды образа "Свой" имеют очень низкую энтропию (1) на уровне 0,1 бита. Коды образа "Чужой", напротив, могут иметь энтропию в 500 раз больше (2) (на уровне 50 бит). Логично предположить, что образы "Чужой" с минимальной энтропией будут ближе к образу "Свой" в сравнении с образами "Чужой", имеющими высокую энтропию. Следовательно, оценивая энтропию образов "Чужой", можно направленно двигаться в сторону образа "Свой".

Вычисление энтропии следует начинать с определения центра кодов образа "Чужой-*k*". Блок-схема таких вычислений проиллюстрирована на рис. 3.

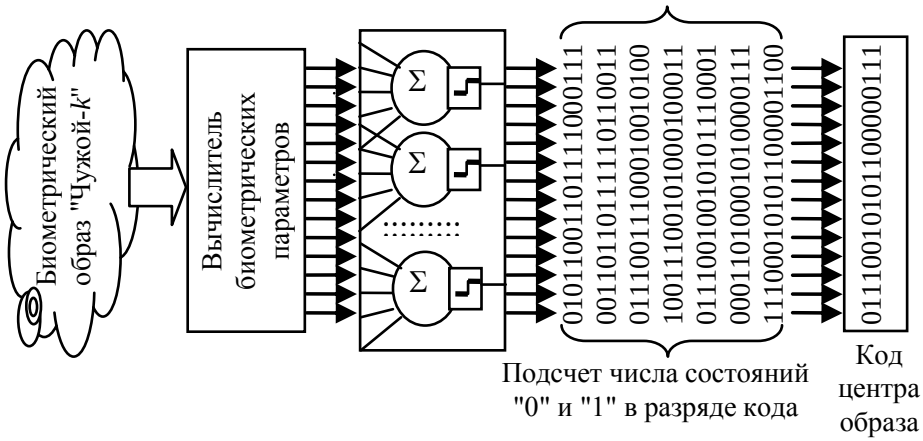

Рис. 3. Блок-схема вычисления центра кодов образа "Чужой-k"

В соответствии с блок-схемой на рис. 3 на входы обученной нейросети подают примеры образа "Чужой-*k*". Каждый пример приводит к появлению на выходах нейросети нового кодового состояния. Далее выполняют подсчет состояний "0_i" и состояний "1_i" в каждом *i*-м разряде кода. Код центра вычисляют по следующему правилу:

$$\begin{cases} E("x_i") \leftarrow "0_i" \text{ при } \sum "0_i" \geq \sum "1_i"; \\ E("x_i") \leftarrow "1_i" \text{ при } \sum "0_i" < \sum "1_i". \end{cases} \quad (3)$$

Далее следует для кодового центра образа "Чужой-*k*" вычислить расстояния Хэмминга для "Всех Чужой" по правилу

$$"h" = \sum_{i=1}^{256} "z_i" \oplus E("x_i"), \quad (4)$$

где "z_i" — кодовые состояния разрядов одного из примеров образа "Чужой-*j*" ($k \neq j$);

$\oplus$ — символ операции сложения по модулю два.

При вычислении суммы из 256 случайных состояний (4) происходит нормализация распределения расстояний Хэмминга, как это показано на рис. 4. Достаточно от 20 до 30 случайно выбранных примеров "Чужой-*j*" для вычисления математического ожидания $E("h")$ и стандартного отклонения $\sigma("h")$ распределений Хэмминга биометрических образов "Чужой-*k*", "Чужой-*k* + 1", "Чужой-*k* + 2", …

Энтропию для каждого биометрического образа "Чужой-*k*" вычисляют в рамках гипотезы нормального закона распределения значений по следующей формуле:

$$H("x_{001}, x_{002}, ..., x_{256}") = \\ = -\log_2 \left\{ \frac{1}{\sigma("h")\sqrt{2\pi}} \int_0^1 \exp\left[\frac{-\left(E("h") - u\right)^2}{2\left(\sigma("h")\right)^2} \right] du \right\}. \quad (5)$$

Поскольку можно вычислить значения кодовых центров $E("x_i")$ всех образов "Чужой" и значения их энтропий $H("\bar{x}_i")$, можно их взаимно упорядочить по этим двум параметрам. Пример такого взаимного упорядочивания приведен на рис. 5.

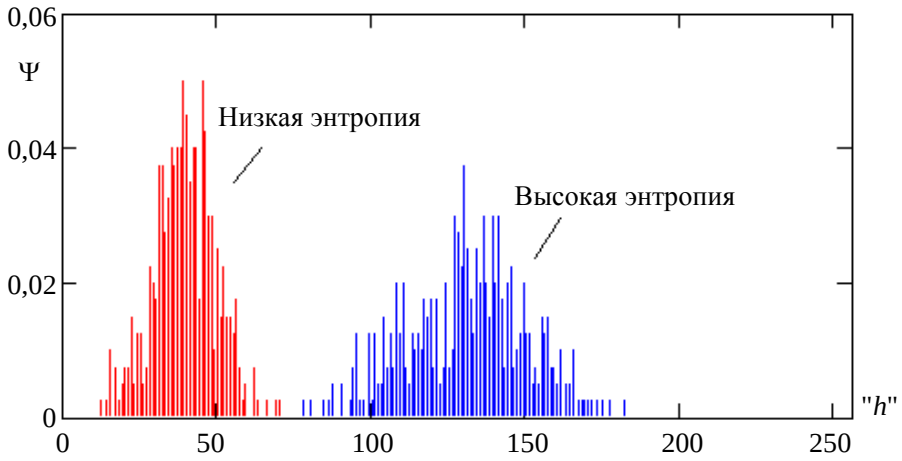

Рис. 4. Амплитуды вероятности появления спектра линий расстояний Хэмминга для близких и далеких образов "Чужой"

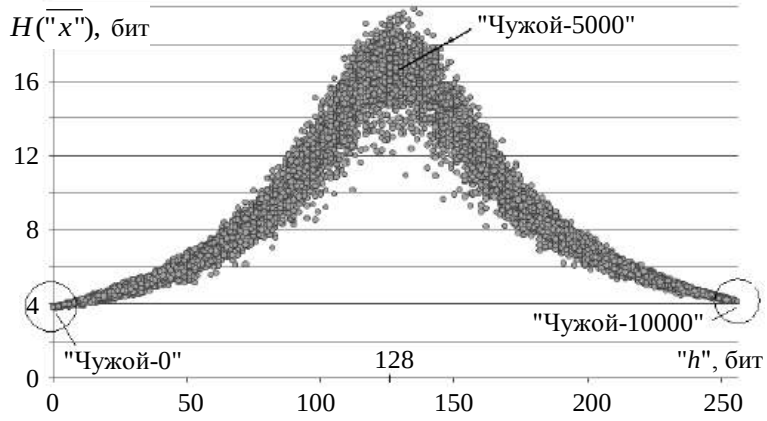

Рис. 5. Пример распределения энтропии упорядоченных образов "Чужой"

Данные, отображенные на рис. 5, получены поиском образа "Чужой" с минимальным значением энтропии $\min\{H("\bar{x}")\}$. Далее этому образу присвоен нулевой номер "Чужой-0". Все другие образы из тестовой базы также следует перенумеровать, обеспечивая монотонное увеличение расстояний Хэмминга между кодовыми центрами образов "Чужой-0" и "Чужой-*k*".

Из рис. 5 видно, что упорядоченное распределение энтропий образов "Все Чужие" имеет две группы образов с минимальными значениями энтропии. Левая группа имеет кодовые центры, близкие к кодовому центру "Чужой-0". Правая группа образов "Чужой" с минимальным значением энтропии имеет предельное расстояние Хемминга от их центров до центра "Чужой-0" 256 бит. У сетей нейронов с линейным накоплением данных один из минимумов энтропии будет объединять образы "Чужой" с центрами, близкими к коду ключа "Свой", второй — объединять вокруг себя образы "Чужой", центры которых близки к инверсии кода ключа "Свой".

Пользуясь этим свойством, атакующий выбирает из первого (нулевого) минимума энтропии 101 образ {"Чужой-0", "Чужой-1", …, "Чужой-100"}. Далее следует восстановить численность базы "Чужой" для вычисления во втором поколении. Формально следует, воспользовавшись рекомендациями ГОСТ Р 52633.2-2010, получить из каждой пары образов-родителей один образец-потомок. Усреднение биометрических параметров двух образов-родителей дает один образ-потомок, одинаково похожий на своих родителей. Подсчет пар образов-родителей по объему выборки выполняют по следующей формуле:

$$\sum_{i=0}^{100}(100-i)=5050. \qquad (6)$$

На рис. 6 дано символьное отображение операции восстановления численности правой и левой части прореженной базы образов "Чужой".

Из рис. 5 видно, что в первом поколении средняя энтропия 10 000 образов "Чужой" составляет примерно 11 бит, а после прореживания средняя энтропия 100 образов "Чужой" в левой и правой выборках составляет примерно 4 бита. После восстановления численности образов "Чужой" (морфинг-скрещиванием по ГОСТ Р 52633.2-2010) с учетом мутаций в 5 % от естественной нестабильности биометрических данных средняя энтропия второго поколения составляет порядка 6,4 бит для 10 000 образов "Чужой" (см. рис. 6).

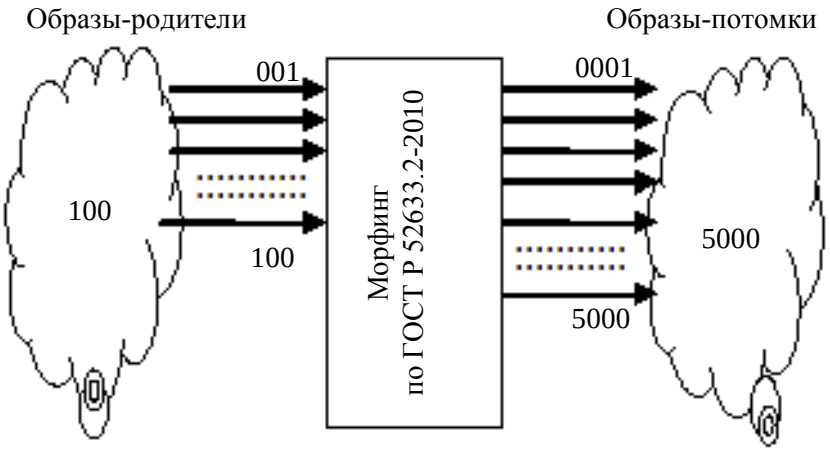

Рис. 6. Морфинг-восстановление численности примеров прореженной базы образов "Чужой" до первоначальной по ГОСТ Р 52633.2-2010

Минимальная энтропия 100 отсортированных образов во втором поколении составляет 2,7 бита. Происходит монотонное снижение энтропии биометрических образов в каждом следующем поколении. Примерно после 50 поколений вычислений среднее значение энтропии образов становится близким к энтропии образа "Свой" и составляет порядка 0,3 бит. При этом удается восстановить до 97 % разрядов кода "Свой" и до 97 % биометрических параметров. Проводимые вычисления занимают примерно 10 мин времени при использовании обычной вычислительной машины с объемом оперативной памяти не менее 1 Гбайта.

Оценка ускорения вычислений, полученного за счет модуляции данных на входе исследуемой сети искусственных нейронов

Среда моделирования БиоНейроАвтограф позволяет наблюдать (запоминать) биометрические параметры рукописного образа в виде файла "params.txt" объемом 3,2 Кбайта. Соответственно 20 примеров образа "Чужой" занимают 64,0 Кбайта. Тестовая база на 10 000 биометрических образов "Чужой" занимает 640 Мбайтов оперативной памяти.

Для быстрого выполнения описанных в данной работе вычислений необходимо использовать вычислительную машину с объемом оперативной памяти в 1 Гбайт и более. Программное обеспечение решаемой задачи и тестовая база из 10 000 образов "Чужой" должны размещаться в оперативной памяти, программное обеспечение решения задачи обращается к долговременной памяти. Обращение к долговременной памяти снижает время вычисления примерно в 1000 раз, т. е. вычислительная машина с объемом памяти 100 Мбайт вместо 10 мин машинного времени будет решать задачу 10 000 мин (примерно 7 суток).

Еще одним важным моментом, обеспечивающим ускорение вычислений, является то, что мы не создаем заранее большую базу искусственных биометрических образов. Это технически невозможно. Если пойти этим путем, то придется уже во втором поколении создавать примерно $(5\,000)^2\times$ $\times 64$ Кбайт = $1{,}6\times10^9$ Кбайт = 1 600 000 Гбайт информации. С такой памятью нет массово выпускаемых недорогих компьютеров. Обычный магнитный диск имеет объем 160 Гб памяти.

Авторам удалось решить поставленную задачу по извлечению знаний из таблиц обученной сети искусственных нейронов только потому, что они в каждом поколении снижали объем памяти в 50 раз и сокращали объем вычислений в 50 раз. Общий объем сокращения памяти и сокращения вычислений составил 50^{50} раз в 50 поколениях (или "полугугл" ускорения).

Решаемая задача может быть усложнена, если увеличить число нейронов до 512. В этом случае число поколений в первом приближении должно удвоиться, т. е. будет иметь место ускорение в 50^{100} раз. При этом время вычислений должно удвоиться и составить порядка 20 мин машинного времени. При переходе к извлечению знаний из нейронной сети с 1024 выходами происходит еще одно удвоение показателя степени до величины 50^{200} раз. Это означает, что задача извлечения знаний из нейронной сети с 1024 выходами по рассмотренному алгоритму обеспечивает ускорение вычислений в "гугл" раз ($50^{200}=100^{100}$).

Заключение

Таким образом, перевод исследования большой сети искусственных нейронов из статики в динамику позволяет наблюдать спектральные линии Хэмминга. Такой переход, в свою очередь, позволяет экспоненциально сократить число анализируемых состояний нейросети. Так, число выходных состояний нейросети с 256 выходами огромно (2^{256}). Отображение описания нейросети в пространство расстояний Хемминга снижает число состояний всего до 257. Именно переход в пространство расстояний Хэмминга в конечном итоге и позволяет получать ускорение вычислений в "полугугл" или полный "гугл".

С другой стороны, относительная простота алгоритма извлечения знаний, размещенных в таблицах нейросети, компрометирует нейросетевую защиту персональных биометрических данных. Нельзя хранить данные таблиц обученных нейронных сетей открыто. Безопасным являются хранение и транспорт нейронных сетей с криптографически защищенными таблицами связей и таблицами весовых коэффициентов [7]. При этом требования к реализации криптографических механизмов, используемых технической спецификацией [7], много ниже, чем требования к таким же криптографическим механизмам по международным стандартам ISO/IEC JTC1 sc27.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 6

Литература

1. *Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Сеньор Эндрю У.* Руководство по биометрии / пер. с англ. — М.: Техносфера, 2007. — 368 с.

2. *Ахметов Б. С., Иванов А. И., Фунтиков В. А., Безяев А. В., Малыгина Е. А.* Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа. — Алматы: ТОО "Издательство LEM", 2014 г. — 144 с. http://portal.kazntu.kz/files/publicate/2014-06-27-11940.pdf

3. *Juels A., Wattenberg M.* A Fuzzy Commitment Scheme: Proc. ACM Conf. Computer and Communications Security, Singapore — November 01—04, 1999. P. 28—36.

4. *Monrose F., Reite M., Li Q., Wetzel S.* Cryptographic key generation from voice: Proc. IEEE Symp. on Security and Privacy, Oakland, CA, USA, 14—16 May, 2001. P. 202—213.

5. *Чморра А. Л.* Маскировка ключа с помощью биометрии // Проблемы передачи информации. 2011. № 2(47). С. 128—143.

6. *Иванов А. И., Захаров О. С.* Среда моделирования "БиоНейроАвтограф" [Электронный ресурс]. Режим доступа: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip

7. Техническая спецификация "Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов". Находится на этапе публичного обсуждения ТК 26 Госстандарта России.

Evaluation of computation acceleration in the mode of program playback of the effects of neurodynamics when extracting knowledge from large networks of artificial neurons

A. I. Ivanov
Penza Research Electrotechnical Institute, Penza, Russia

A. I. Gazin
Lipetsk Pedagogical University named after P. P. Semenova-Tyan-Shanskogo, Lipetsk, Russia

A. E. Sulavko, D. G. Stadnikov
Omsk State Technical University, Omsk, Russia

The article deals with the estimation of acceleration obtained by modulation of input artificial neurons in accordance with the requirements of seven domestic standards of GOST R 52633.xxx series. Modulation of input data of the investigated network of artificial neurons by crossing biometric parent-images and obtaining biometric parent-images from them in accordance with GOST R 52633.2-2011 is used.

Keywords: artificial neurons, big data, input data modulation, neurodynamics.

Bibliography — 7 references. *Received November 25, 2020*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056.5

Математический аппарат для описания модели нарушителя в системах защиты

Д. В. Титов, канд. техн. наук; *Е. Е. Филипова*, канд. физ.-мат. наук
ФКОУ «Вологодский институт права и экономики ФСИН России», г. Вологда, Россия

Рассмотрена задача снижения риска преодоления потенциальным нарушителем систем защиты информации в информационных системах, сложность которой определяется прежде всего тем, какая система уравнений будет использована для ее описания и, следовательно, выбора метода решения.

Ключевые слова: система, защита, надежность, программное обеспечение, вероятность, байесовский подход, математическая модель, атака, уязвимость, модель нарушителя.

В информационных системах присутствует риск преодоления систем защиты потенциальным нарушителем. Описание и прогнозирование его действий являются актуальной задачей. Это связано с преодолением кризиса, который испытывают специалисты в области информационной безопасности в связи с резким увеличением количества атак на системы защиты информационных систем организаций и учреждений. Способы, используемые нарушителями во время "коронавирусной" информационной войны, — это, как правило, постоянный поиск уязвимых мест, непрерывные сетевые атаки, отвлекающие вторжения и т. п.

Задача формируется следующим образом. Процесс функционирования системы тесно связан с набором функций, ее математическим описанием, однозначно определяющим систему защиты во времени. Вместе с тем необходимо искусственно создать модель нарушителя с определенным уровнем адекватности модели реальному объекту.

Надежность систем защиты определяется набором свойств, позволяющих говорить о способности системы противостоять внешним атакам. В первую очередь нужно выделить наиболее уязвимые объекты. Такими объектами являются программы, отвечающие за первичную защиту, т. е. программы-мониторы, сетевые экраны и т. п. Таким образом, нужно рассматривать надежность системного программного обеспечения и вероятность отказа (ошибки) его функционирования.

Рассмотрим математические методы, которые можно использовать для оценки вероятности отказа программного обеспечения и снижения уровня защиты системы.

Построим модель оценки вероятности отказов на основе теории Байеса.

Определив переменные, составим функцию для описания модели потенциального нарушителя. Выделим следующие:

- киберугрозы X_1;
- потенциальный ущерб от действий нарушителя X_2;
- степень уязвимости информационной системы X_3.

В государственном учреждении, как правило, разрабатывают перечень мероприятий, направленных на обеспечение уровня информационной безопасности. Обозначим влияние данных мероприятий, как фактор, через X_4.

Для количественного определения риска информационной безопасности представим его в виде функции

$$R = f\left(X_1, X_2, X_3, X_4\right). \qquad (1)$$

Для математической формализации моделей защиты информации в подобных системах используют различные модели и методы. Одним из способов служат байесовские сети. В основе байесовских сетей лежит теорема Байеса. Теорема Байеса позволяет пересчитать вероятности событий, вме-

Титов Дмитрий Валерьевич, доцент кафедры "Информатика и математика" факультета психологии и права.
E-mail: titov_dv@mail.ru
Филипова Елена Евгеньевна, доцент кафедры "Информатика и математика" инженерно-экономического факультета.
E-mail: lenphil@mail.ru

Статья поступила в редакцию 2 декабря 2020 г.

сте с которыми может наступить некоторое рассматриваемое событие, при условии его свершения. Выгодным свойством использования байесовского подхода является тот факт, что имеющаяся в распоряжении экспертов информация может и не отвечать требованиям представительности статистической выборки. Таким образом, в качестве одного из возможных примеров можно рассматривать использование подхода Байеса [2].

Для иллюстрации байесовского подхода определим основные показатели защищенности системы. Далее присвоим этим показателям 1-й, 2-й и 3-й классы соответственно:

1. Система обеспечивает конфиденциальность информации при воздействии угрозы y_1.

2. Система способна обеспечить целостность информации y_2.

3. Система должна обеспечить доступность информации y_3.

Постановка задачи. Пусть из возможного числа типовых киберугроз известно, что при воздействии на информационные ресурсы 1-го класса система защиты информации выдерживала атаки в 50 % случаев, 2-го — в 70 %, 3-го — в 5 %. Отсюда определяем условные вероятности:

$$P_1(y_1) = 0,5;$$
$$P_2(y_2) = 0,7;$$
$$P_3(y_3) = 0,05.$$

Аналогично условные вероятности могут быть определены для 2-го и 3-го классов при исследовании надежности системы защиты информации.

Применение байесовского подхода помогает также решить вопрос о математических методах оценивания априорных значений, которые могут принимать параметры риска информационной безопасности. Вместе с тем для оценки риска нарушения информационной безопасности целесообразно выбирать распределение, минимально влияющее на апостериорное [3].

Таким образом, модель нарушителя выглядит так. В случае реализации угрозы безопасности сети нарушитель разрабатывает сценарий атаки, использующий одну уязвимость. При этом нарушение безопасности происходит путем эксплуатации наибольшей уязвимости. В случае, если несколько уязвимостей равноценны, из них выбирают одну произвольную [3].

Построим математическую модель. Введем следующие обозначения:

- L — возможная угроза информационной безопасности системы;
- $p(L)$ — вероятность успешной реализации угрозы;
- $I_1, I_2, ..., I_n$ — набор уязвимостей, несовершенство программного обеспечения и т. п.;
- $p(I_1), ..., p(I_n)$ — вероятности захвата управления программами защиты вследствие негативного использования уязвимостей.

Условно обозначим через S величину, которая будет показывать оснащенность нарушителя, т. е. имеющийся "арсенал атаки".

Следует считать, что возможны два варианта развития:

– $S \le p(I_i)$ (угроза не наступает или реализуется с минимальными потерями для систем защиты);

– $S \ge p(I_i)$ (угроза наступает или приводит к максимальному ущербу, деактивации системы защиты, частичной потере функций специального программного обеспечения, реализации атаки).

Заключение

В заключение отметим, что использование моделей потенциального нарушителя систем защиты для оценки эффективности систем защиты является тем инструментом, который позволяет прогнозировать состояние системы при наступлении тех или иных неблагоприятных событий. Процесс испытания системы защиты на данных моделях позволяет минимизировать количество ошибок системы, выявить на ранних стадиях уязвимые места в программных кодах, составе и модулях системного программного обеспечения. В конечном итоге это позволит упреждать, а также оценивать возможные потери от действий нарушителей системы защиты в организации или учреждении.

Литература

1. *Зикратов И. А., Одегов С. В.* Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4(80). С. 121—126.

2. *Атаманов А. Н.* Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах: дисс. … канд. техн. наук. — М.: Нац. исслед. ядерный ун-т, 2012.

3. *Титов Д. В., Филипова Е. Е.* Применение математических моделей оценки риска киберугроз для обеспечения информационной безопасности: сб. мат. науч.-практ. семинара "Современные средства автоматизации деятельности сотрудников территориальных органов и образовательных организаций ФСИН России: проблемы и перспективы" Вологда, 24 октября 2019 г. / под. ред. Бабкина А. А. — Вологда: ВИПЭ ФСИН России, 2020. — 178 с.

Mathematical apparatus for describing the model of intruder in protection systems

D. V. Titov, E. E. Filipova
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia,
Vologda, Russia

Reducing the risk of a potential violator of information protection systems in information systems is a task whose complexity is determined primarily by which system of equations will be used to describe it and, therefore, select a solution method.

Keywords: system, protection, reliability, software, probability, Bayesian approach, mathematical model, attack, vulnerability, intruder model.

Bibliography — 3 references. *Received December 1, 2020*

УДК 519.24; 53; 57.017

Проверка гипотезы независимости малых выборок: воспроизведение эффектов нейродинамики через случайное прореживание исходных данных

А. И. Иванов, д-р техн. наук
АО «Пензенский научно-исследовательский электротехнический институт», г. Пенза, Россия

Т. А. Золотарева
ФБГОУ ВО «Липецкий педагогический университет им. П. П. Семенова-Тян-Шаньского», г. Липецк, Россия

А. Е. Сулавко, канд. техн. наук; *А. Г. Чобан*
ФГБОУ ВО «Омский государственный технический университет», г. Омск, Россия

Проанализированы малые выборки по нескольким статистическим критериям проверки гипотезы независимости, так как прямое вычисление коэффициентов корреляции по формуле Пирсона дает неприемлемо высокую погрешность. Предложено каждый из классических статистических критериев проверки гипотезы независимости заменить эквивалентным ему искусственным нейроном. Обучение нейрона выполняется исходя из условия получения равных вероятностей ошибок первого и второго рода. Кроме того, для повышения уровня достоверности принимаемых нейросетью решений предложено использовать модуляцию путем прореживания и перестановок данных исходной малой выборки. Это позволяет наблюдать спектральные линии расстояний Хэмминга последовательности выходных кодов сети искусственных нейронов.

Ключевые слова: искусственные нейроны, критерии проверки гипотезы независимости, малые выборки, модуляция входных данных нейросети.

При обработке малых выборок реальных данных биометрии, биологии, медицины, экономики часто требуется вычислить коэффициент корреляции $r(x, y)$ между двумя последовательностями. Когда выборки реальных данных велики и составляют 100 и более опытов, вычисление коэффициентов корреляции может быть выполнено по формуле Пирсона.

К сожалению, в биометрии выборок столь значительного объема не бывает. Так, нейросетевой преобразователь биометрии в длинный код автоматически обучается на 16—20 примерах образа "Свой" алгоритмом ГОСТ Р 52633.5-2011. Это означает, что на выборках от 16 до 20 опытов нужно уметь достаточно точно вычислять математические ожидания, стандартные отклонения и коэффициенты корреляции биометрических параметров. При расчетах ошибки промежуточных вычислений накапливаются. Формально ошибка коэффициента корреляции является функцией нескольких переменных: $\Delta r\{x, y, \Delta[E(x)], \Delta[E(y)], \Delta[\sigma(x)], \Delta[\sigma(y)]\}$, где $\Delta(...)$ — ошибка вычислений; $E(...)$ — операция вычисления математического ожидания; $\sigma(...)$ — операция вычисления стандартного отклонения.

Практика показывает, что с уменьшением объема выборки ошибки вычислений всех параметров растут. При вычислении коэффициентов корреляции по формуле Пирсона для выборок в 16 опытов получим распределения, отображенные на рис. 1.

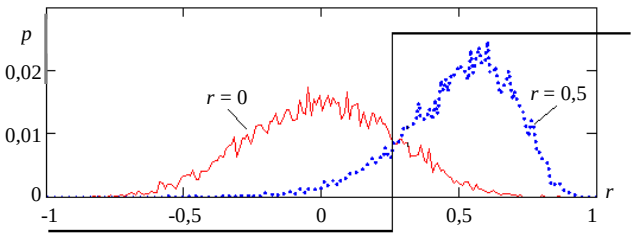

Рис. 1. Распределение выходных состояний нейрона Пирсона, обученного распознавать выборки по 16 опытов без корреляции (r = 0) и выборки по 16 опытов с высоким

Иванов Александр Иванович, доцент, научный консультант.
E-mail: bio.ivan.penza@mail.ru; ivan@pniei.penza.ru
Золотарева Татьяна Александровна, старший преподаватель.
E-mail: sulavich@mail.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Чобан Адиль Гаврилович, инженер-программист.
E-mail: adil_choban@mail.ru

Статья поступила в редакцию 25 ноября 2020 г.

значением корреляции (r = 0,5)

Из рис. 1 видно, что для независимых данных вычисления по формуле Пирсона на выборке в 16 опытов могут давать значения, попадающие в интервал от -0,75 до +0,75. Если же работать с данными, имеющими коэффициент корреляции 0,5, то формула Пирсона будет давать значения в интервале от -0,25 до 1,0.

Все это делает очень проблематичным вычисление первых статистических моментов биометрических данных по малым выборкам. Хорошо, что часть задач биометрии не требует точного знания значений коэффициентов корреляции (третьих статистических моментов). Во многих случаях статистического анализа [1—4] можно ограничиться выбором независимых биометрических данных. При этом можно воспользоваться десятками известных статистических критериев, созданных в прошлом веке [5] для проверки гипотезы независимости:

- Пирсона;
- Пирсона—Эджуорта—Эудлона;
- Спирмена;
- Нельсона и т. д.

Очевидно, что каждый из известных статистических критериев проверки гипотезы независимости будет иметь свое значение ошибок первого и второго рода. Каждый критерий будет порождать свою нелинейную шкалу оценок. Если попытаться совместно применить несколько статистических критериев, то придется каким-то образом совмещать между собой различные шкалы. Последнее является крайне трудной в вычислительном отношении задачей.

Нейросетевое обобщение различных статистических критериев

Уйти от проблемы совмещения множества нелинейных шкал удается, если каждому из известных статистических критериев поставить в соответствие эквивалентный ему искусственный нейрон. В частности, для формулы Пирсона и выборки в 16 опытов эквивалентный искусственный нейрон будет описываться следующими функциональными связями:

$$\begin{cases} r \leftarrow \sum_{i=0}^{15}\left[x_i - E(x)\right]\left[y_i - E(y)\right] \Big/ 16\,\sigma(x)\,\sigma(y); \\ z(r) \leftarrow \text{"0"} \ \text{при} \ r \le 0,25; \\ z(r) \leftarrow \text{"1"} \ \text{при} \ r > 0,25. \end{cases} \quad (1)$$

На рис. 1 отображены два состояния выходного квантователя нейрона (1). При отклике сумматора нейрона менее порога квантователя 0,25 нейрон выдает состояние "0", соответствующее обнаружению независимых данных. При выходном значении сумматора искусственного нейрона Пирсона более 0,25 нейрон выдает состояние "1", соответствующее обнаружению выборки с зависимыми данными.

Следует подчеркнуть, что порог компаратора $r = 0,25$ специально выбирают таким образом, чтобы ошибки первого и второго рода были одинаковыми: $P_1 \approx P_2 \approx P_{EE} \approx 0,164$. В этом случае удается достаточно легко симметризовать задачу совмещения разнородных нелинейных шкал разных статистических критериев [6, 7].

В качестве еще одного критерия рассмотрим показатель Херста [8, 9]. Соответствующий этому показателю искусственный нейрон описывается следующими функциональными связями:

$$\begin{cases} R(\tilde{x}, \tilde{y}) \leftarrow R\left[\text{sort}(x), y\right]; \\ rX \leftarrow \left[\max(\tilde{y}) - \min(\tilde{y})\right] / \sigma(\tilde{y}); \\ z(rX) \leftarrow \text{"0"} \ \text{при} \ rX \le 1,13; \\ z(rX) \leftarrow \text{"1"} \ \text{при} \ rX > 1,13. \end{cases} \quad (2)$$

Вычисления построены на том, что исходную выборку подвергают сортировке. По итогам сортировки пары $\{x_i, y_i\}$ должны дать монотонный рост сортируемой переменной $\tilde{x}_i \le \tilde{x}_{i+1}$. Показатель Херста вычисляют как отношение размаха немонотонной части отсортированной последовательности $\{\tilde{y}_0, \tilde{y}_1, ..., \tilde{y}_{15}\}$ к ее стандартному отклонению. Выходные состояния искусственного нейрона Херста отображены на рис. 2.

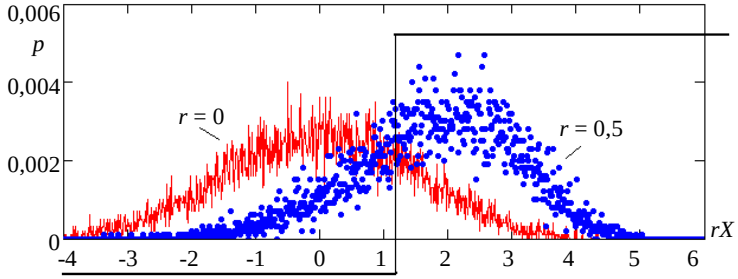

Рис. 2. Выходные состояния нейрона Херста, обученного различать независимые и зависимые данные с вероятностями ошибок $P_1 \approx P_2 \approx P_{EE} \approx 0,224$

Получается, что искусственный нейрон Херста дает примерно в полтора раза большие значения вероятностей ошибок в сравнении с нейроном Пирсона, однако их выходные состояния имеют значительную независимую компоненту $\mathrm{corr}(r, rX) \approx 0,651$. Если бы корреляция выходных состояний этих двух нейронов была полной $|\mathrm{corr}(r, rX)| = 1,0$, то пользоваться этой парой нейронов было бы бесполезно. Неполная корреляция их выходных состояний $|\mathrm{corr}(r, rX)| < 1,0$ позволяет утверждать, что их совместное использование выгодно.

Решения, принимаемые 7 нейронами с использованием простейшего кода обнаружения и исправления ошибок

Формально можно предположить, что все статистические критерии, разработанные в прошлом веке, будут иметь похожие вероятности ошибок первого и второго рода и будут связаны примерно так же, как два рассмотренных нейрона. При выполнении симметризации [6, 7] необходимо вычислить среднее геометрическое вероятностей ошибок первого и второго нейронов:

$$P_1 \approx P_2 \approx P_{EE} \approx \sqrt{0,164 \cdot 0,224} \approx 0,192. \qquad (3)$$

Далее предположим, что удалось создать сеть из 7 искусственных нейронов, связанных между собой матрицей одинаковой коррелированности $\mathrm{corr}(z_i, z_j) = 0,651$ для $i \neq j$. Такая сеть искусственных нейронов легко моделируется и должна давать состояние "0000000" (7 разрядов с состоянием "0") в случае, когда с высокой вероятностью все нейроны обнаруживают независимую выборку. В случае, если все нейроны дают состояние "1", то с очень высокой вероятностью можно говорить об обнаружить выборки с коэффициентом корреляции $r \approx 0,5$ и выше.

Ситуации, когда выходной код нейросети состоит только из "0" или только из "1", легко интерпретировать, однако обычно наблюдаются различные случайные комбинации состояний "0" и состояний "1" в разных разрядах. Для получения однозначного решения необходимо свернуть все состояния кода к одному состоянию. Например, это может быть сделано подсчетом числа состояний "0". Если число состояний "0" больше числа состояний "1", принимается решение об обнаружении слабо коррелированной малой выборки. Более сложные коды, корректирующие ошибки нейросетевых преобразователей биометрия—код, рассмотрены в работе [10].

Следует подчеркнуть, что статистический анализ достаточно длинных кодов, состоящих из 7 разрядов с почти случайным расположением состояний "0" и "1", является сложной технической задачей. Упростим эту задачу, перейдя от анализа исходных кодов к анализу их расстояний Хэмминга до идеального кода, состоящего из одних нулей:

$$H(\text{"}\bar{0}\text{"}) = \sum_{i=1}^{7} (\text{"0"}) \oplus (\text{"}z_i\text{"}), \qquad (4)$$

где "z_i" — состояние i-го разряда анализируемого кода;

$\oplus$ — операция сложения по модулю два.

Упрощения, связанные с переходом в пространство расстояний Хэмминга, обусловлены тем, что число возможных состояний исходных кодов составляет $2^7 = 128$, а в пространстве расстояний Хэмминга число состояний снижается до 8. На рис. 3 представлены амплитуды вероятности 8 спектральных линий Хэмминга.

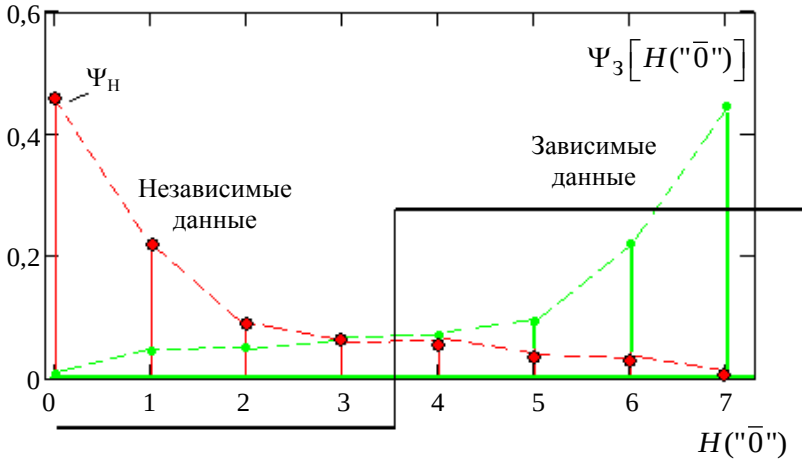

Рис. 3. Амплитуды вероятности появления восьми спектральных линий Хэмминга для семиразрядных кодов симметризованной нейросети

Если принимать решение об обнаружении нормальных данных по большинству нулей, то равновероятная ошибка после корректировки составит $P_1 \approx P_2 \approx P_{EE} \approx 0{,}154$, что лучше исходного среднего геометрического вероятностей $0{,}192/0{,}153 \approx 1{,}26$ примерно на 26 %. Таким образом, наблюдается незначительное снижение вероятностей ошибок из-за применения семи статистических критериев.

Можно показать, что увеличение числа искусственных нейронов до 9, 11, 13 и так далее всегда будет приводить к монотонному снижению вероятностей ошибок принимаемого решения. Однако снижение вероятностей ошибок оказывается медленным из-за сильной коррелированности выходных состояний искусственных нейронов.

Повышение качества принимаемых нейросетевых решений за счет модуляции данных малой выборки перестановками и прореживанием

При подаче одной малой выборки в 16 опытов на входы 7 искусственных нейронов получается единственный выходной код. Как результат нельзя наблюдать амплитуды вероятности спектральных линий Хэмминга, показанные на рис. 3. Положение меняется при использовании выборки чуть больших размеров, например состоящей из 21 опыта. В этом случае можно сформировать порядка 20 000 малых подвыборок по 16 опытов путем перестановки данных и извлечения из них по 5 опытов. Такого типа преобразования описывают биномиальными соотношениями:

$$C_n^k = C_{21}^{16} = \frac{n!}{k!(n-k)!} = \frac{21!}{16!(21-16)!} = 20349 .$$

Фактически мы создаем некоторый модулятор, который меняет входные данные анализируемой выборки.

В случае, когда на нейросетевой преобразователь (рис. 4) подают одну выборку в 21 опыт нормально распределенных данных, выходное состояние кода из одних единиц возникает крайне редко, $\Psi_{\text{Н}}(\text{"1111111"}) \approx 0{,}0096$. Столь же редким событием является появление в коде всех нулей, если на нейросеть подаются зависимые данные $\Psi_{\text{З}}(\text{"0000000"}) \approx 0{,}0082$. Оценка даже самых малых амплитуд вероятности спектральных линий Хэмминга для нейросети из 7 нейронов вполне может быть выполнена на 20 000 выборок по 16 опытов. Все иные амплитуды вероятностей спектральных линий существенно больше. Соответственно для их оценки потребуются выборки меньшего объема.

Поскольку происходит переход от анализа нейростатики к анализу нейродинамики, можно применить для классификации зависимых и независимых данных второй слой нейронов, обученных распознавать два разных спектра: $\Psi_{\text{Н}}(\text{"…"})$ и $\Psi_{\text{З}}(\text{"…"})$. Такой подход технически возможен, но связан со значительными затратами на программирование (не является доказательным).

Убедительным является иной подход, построенный на усреднении расстояний Хэмминга по 20, 200, 2000 или 20000 выборкам. В этом случае спектр средних расстояний Хэмминга из дискретного превращается в непрерывный.

На рис. 5 представлены подобные спектры, полученные имитационным моделированием.

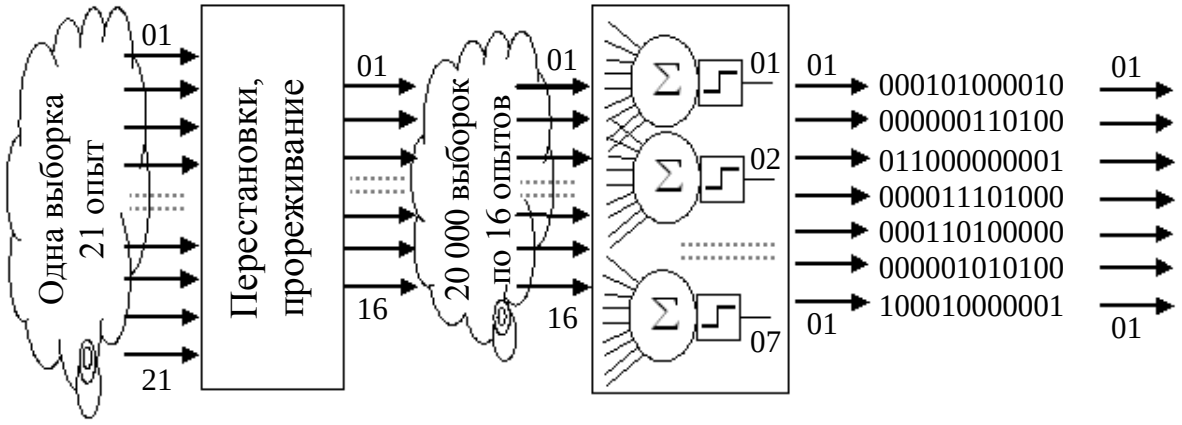

Рис. 4. Размножение данных перестановками и прореживанием из одной выборки в 21 опыт до 20 тысяч подвыборок по 16 опытов

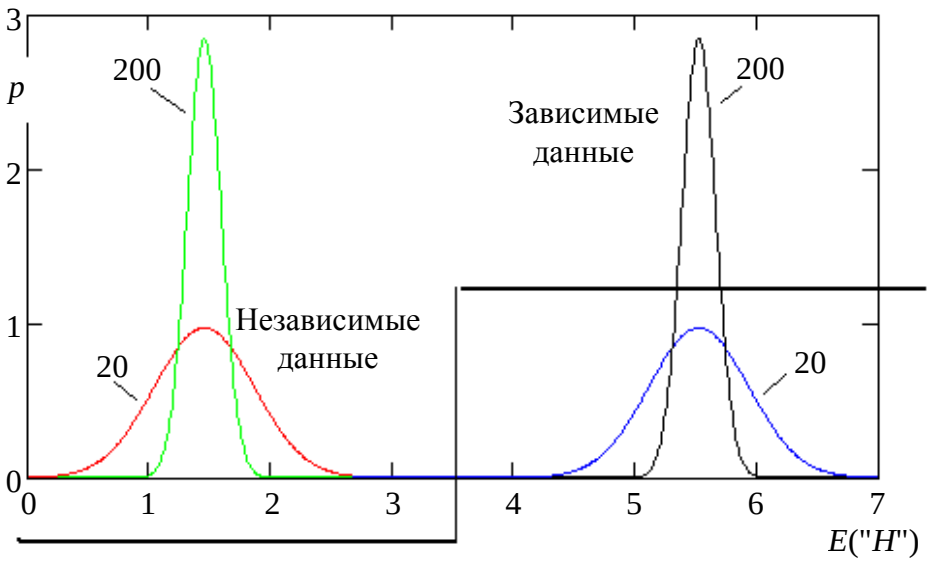

Рис. 5. Аппроксимация спектров математических ожиданий расстояний Хэмминга нормальными распределениями для усреднений по 20 и 200 выборкам

Из рис. 5 видно, что даже усреднение расстояний Хэмминга по 20 выборкам дает снижение вероятности появления ошибок с 0,154 до 0,00000053 (примерно в 300 000 раз). При усреднении по 200 выборкам снижение вероятности ошибок происходит в сотни миллионов раз.

Заключение

В случае применения семи искусственных нейронов, построенных как эквиваленты классических статистических критериев проверки гипотезы независимости и корректировки неоднозначности их выходных кодов в статике, получаем возможность незначительно снизить вероятности появления ошибок (на 26 %). Этого недостаточно для практического применения в биометрии, биологии, медицине, экономике малых выборок реальных данных.

Ситуация кардинально меняется, если перевести сеть искусственных нейронов в динамический режим анализа малых выборок. Переход из нейростатики в нейродинамику позволяет кардинально изменить ситуацию, снижая вероятности ошибок первого и второго рода в сотни тысяч и миллиарда раз. Решающие правила, построенные в нейродинамике, имеют ощутимые преимущества по достоверности принимаемых ими решений на малых выборках.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 6

Литература

1. *Сулавко А. Е., Иванов А. И.* Настройка и балансировка двухмерных гиперболических квантователей Байеса в бинарном исполнении, обеспечивающих равновероятные состояния разрядов выходного кода для образов "Чужой": сб. науч. статей по мат. II Всеросс. онлайн науч.-техн. конф. "Безопасность информационных технологий". — Пенза, 2020. С. 11—15.

2. *Сулавко А. Е.* Биометрическая аутентификация на основе сети гиперболических нейронов Байеса с трехуровневыми квантователями: мат. XI Всеросс. науч.-практ. конф. студентов, аспирантов, работников образования и промышленности "Информационные технологии и автоматизация управления" Омск, 29—30 мая 2020 г. — Омск: ОмГТУ, 2020. С. 199—206.

3. *Ложников П. С.* Биометрическая защита гибридного документооборота. — Новосибирск: Изд-во СО РАН, 2017. — 130 с.

4. *Иванов А. И., Золотарева Т. А.* Искусственный интеллект в защищенном исполнении: синтез статистико-нейросетевых автоматов многокритериальной проверки гипотезы независимости малых выборок биометрических данных: препринт. — Пенза: Изд-во "ПГУ", 2020. — 102 с.

5. *Кобзарь А. И.* Прикладная математическая статистика. Для инженеров и научных работников. — М.: Физматлит, 2006. — 816 с.

6. *Иванов А. И., Банных А. Г., Серикова Ю. И.* Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок // Надежность. 2020. № 20(2). С. 28—34. https://doi.org/10.21683/1729-2646-2020-20-2-28-34

7. *Иванов А. И., Банных А. Г., Безяев А. В.* Искусственные молекулы, собранные из искусственных нейронов, воспроизводящих работу классических статистических критериев // Вестник Пермского университета. Сер. "Математика. Механика. Информатика". 2020. № 1(48). С. 26—32.

8. *Петерс Э.* Хаос и порядок на рынках капитала. Новый аналитический взгляд на циклы, цены и изменчивость рынка / пер. с англ. — М.: Мир, 2000. — 333 с.

9. *Иванов А. И., Егорова Ю. Ю.* Корреляционный метод быстрой оценки текущего значения показателя Херста биометрических данных и данных рынка // Нейрокомпьютеры: разработка, применение. 2012. № 3. С. 26—27.

10. *Безяев А. В.* Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность: препринт. — Пенза: Изд-во Пензенского гос. ун-та, 2020. — 68 с.

Testing the hypothesis of independence of small samples: reproduction of the effects of neurodynamics through random thinning of the source data

A. I. Ivanov
Penza Research Electrotechnical Institute, Penza, Russia

T. A. Zolotareva
Lipetsk Pedagogical University named after P. P. Semenova-Tyan-Shanskogo, Lipetsk, Russia

A. E. Sulavko, A. G. Choban
Omsk State Technical University, Omsk, Russia

The article deals with the analysis of small samples on the basis of several statistical criteria for checking the hypothesis of independence, as direct calculation of correlation coefficients by Pearson formula gives unacceptably high error. It is proposed to replace each of the classical statistical criteria for testing the hypothesis of independence with an equivalent artificial neuron. Training of the neuron is carried out based on the condition of obtaining equal probability of first and second kind errors. In addition, to increase the level of reliability of decisions made by the neural network, it is proposed to use modulation by thinning and rearranging the data of the initial small sample. This makes it possible to observe spectral lines of the Humming distance of the artificial neuron network sequence output codes.

Keywords: artificial neurons, criteria of independence hypothesis verification, small samples, modulation of neuron input data.

Bibliography — 10 references. *Received November 25, 2020*

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас»

……..……
(название журнала)

безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)

…….

…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала.

Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте на CD/DVD-диске с текстом в формате Word.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;

- после названия — список авторов, инициалы авторов предшествуют их фамилиям;
- с отступлением в 2 строки представляется аннотация статьи;
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следую-щих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $v_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ИЗДАТЕЛЬСТВО ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС» ПРЕДЛАГАЕТ:

- ✓ *использовать издания предприятия в качестве информационной площадки Вашей организации;*
- ✓ *осуществлять на регулярной основе публикации в данных журналах научных статей;*
- ✓ *публиковать на страницах изданий*
  - *рекламные и имиджевые материалы Вашей организации;*
  - *обзорные статьи руководителей о последних научно-технических разработках, достижениях, результатах научно-исследовательских работ, проблемах и путях их решений;*
  - *материалы проводимых Вами научно-технических конференций, семинаров и иных отраслевых мероприятий;*
  - *а также любую другую актуальную для Вашей организации информацию, соответствующую тематической направленности журналов.*

ФГУП "Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Издается с 1984 года
ISSN 1729-6552

«Оборонный комплекс — научно-техническому прогрессу России»
научно-технический журнал

Научные специальности журнала:

05.02.02	—	Машиноведение, системы приводов и детали машин;
05.02.05	—	Роботы, мехатроника и робототехнические системы;
05.02.07	—	Технология и оборудование механической и физико-технической обработки;
05.02.13	—	Машины, агрегаты и процессы;
05.02.22	—	Организация производства (по отраслям);
05.12.04	—	Радиотехника, в том числе системы и устройства телевидения;
05.12.07	—	Антенны, СВЧ устройства и их технологии;
05.12.13	—	Системы, сети и устройства телекоммуникаций;
05.12.14	—	Радиолокация и радионавигация;
05.13.06	—	Автоматизация и управление технологическими процессами и производствами (по отраслям);
05.13.10	—	Управление в социальных и экономических системах;
05.13.15	—	Вычислительные машины, комплексы и компьютерные сети;
05.13.18	—	Математическое моделирование, численные методы и комплексы программ.

Издается с 1974 года
ISSN 2073-2600

«Вопросы защиты информации»
научно-практический журнал

Научные специальности журнала:

05.13.01	—	Системный анализ, управление и обработка информации (по отраслям);
05.13.11	—	Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей;
05.13.15	—	Вычислительные машины, комплексы и компьютерные сети;
05.13.18	—	Математическое моделирование, численные методы и комплексы программ;
05.13.19	—	Методы и системы защиты информации, информационная безопасность.

Издается с 1993 года
ISSN 2073-2589

«Экология промышленного производства»
межотраслевой научно-практический журнал

Научные специальности журнала:

05.23.03	—	Теплоснабжение, вентиляция, кондиционирование воздуха, газоснабжение и освещение;
05.23.04	—	Водоснабжение, канализация, строительные системы охраны водных ресурсов;
05.23.19	—	Экологическая безопасность строительства и городского хозяйства;
05.26.06	—	Химическая, биологическая и бактериологическая безопасность.

Издается с 1981 года
ISSN 2073-2562

«Конструкции из композиционных материалов»
межотраслевой научно-технический журнал

Научные специальности журнала:

05.11.01	—	Приборы и методы измерения (по видам измерений);
05.11.07	—	Оптические и оптико-электронные приборы и комплексы;
05.11.08	—	Радиоизмерительные приборы;
05.11.14	—	Технология приборостроения;
05.11.16	—	Информационно-измерительные и управляющие системы (по отраслям);
05.13.05	—	Элементы и устройства вычислительной техники и систем управления;
05.13.06	—	Автоматизация и управление технологическими процессами и производствами (по отраслям);
05.13.10	—	Управление в социальных и экономических системах;
05.13.12	—	Системы автоматизации проектирования (по отраслям);
05.13.15	—	Вычислительные машины, комплексы и компьютерные сети;
05.13.18	—	Математическое моделирование, численные методы и комплексы программ.

Издается с 1976 года
ISSN 2073-2597

«Информационные технологии в проектировании и производстве»

Научные специальности журнала:

05.07.02	—	Проектирование, конструкция и производство летательных аппаратов;
05.07.03	—	Прочность и тепловые режимы летательных аппаратов;
05.07.05	—	Тепловые электроракетные двигатели и энергоустановки летательных аппаратов;
05.07.07	—	Контроль и испытание летательных аппаратов и их систем;
05.16.06	—	Порошковая металлургия и композиционные материалы;
05.17.06	—	Технология и переработка полимеров и композитов;
05.17.11	—	Технология силикатных и тугоплавких неметаллических материалов.

Журналы включены решением ВАК Министерства науки и высшего образования Российской Федерации в перечень ведущих рецензируемых научных журналов и изданий. Метаданные выпусков журнала включены в базу данных Российского индекса научного цитирования (РИНЦ).

Отдел научных и информационных изданий
Тел.: 8 (495) 491-43-17, 8 (495) 491-77-20. *Факс:* 8 (495) 491-44-80.
E-mail: secretariat@ntckompas.ru, izdanie@ntckompas.ru, ivleva@ntckompas.ru

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2021 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Периодич-ность в год	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1550,00		
Конструкции из композиционных материалов	4	1700,00		
Экология промышленного производства	4	1500,00		
Информационные технологии в проектировании и производстве	4	1750,00		
Вопросы защиты информации	4	1750,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:
Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или
E-mail: secretariat@ntckompas.ru
Более подробную информацию об изданиях и подписке можно получить по телефону:
8 (495) 491-43-17, 8 (495) 491-77-20.
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».