ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

(129)

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2020

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

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

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

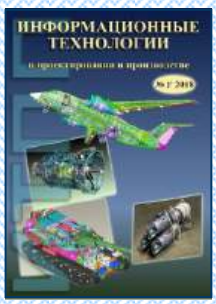
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года

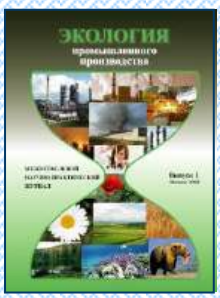


Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года



Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства образования и науки России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: secretariat@ntckompas.ru

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

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

2 (129)

Москва 2020
Основан в 1974 г.

С О Д Е Р Ж А Н И Е

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2020.
Вып. 2 (129). С. 1—76.

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

Подписано в печать 17.06.2020. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 8,8. Уч.-изд. л. 9,1.
Тираж 400 экз. Заказ 1953. 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 621.372.552

Метод встраивания информации в младшие биты растровых изображений без сжатия, использующий двухкомпонентный контейнер

М. В. Шакурский, канд. техн. наук
Самарский государственный технический университет, Самара, Россия

Рассмотрен метод встраивания информации в младшие биты растрового изображения без сжатия с предварительной маскировкой сообщения случайным сигналом. Маскировка сообщения осуществляется с помощью алгоритма сокрытия информации на основе суммы линейных функций двух сигналов, использующего аддитивный вид связи встраиваемых сигналов.

Ключевые слова: двухкомпонентная стеганографическая система, инвариантность от маскирующего сигнала, стеганографический контейнер, ключевой коэффициент, растровое изображение, метод наименьших значащих бит.

Совершенствование систем стеганографии связано с их быстродействием, минимизацией информации, необходимой для извлечения скрытого сигнала, и устойчивостью к целенаправленному или слепому стеганографическому анализу. В работах [1—10] рассмотрен новый подход к формированию стеганографического контейнера в виде двух компонент, позволяющий получить новые свойства стеганографических систем. В работе [1] рассмотрен алгоритм формирования компонент стеганографической системы на основе суммы линейных функций двух сигналов, в [2—10] — нелинейные алгоритмы формирования компонент. Извлечение сообщений в таких системах происходит без знания сигнала контейнера. Встраивание компонент осуществляют за счет преобразования отсчетов контейнера. При этом в отличие от метода наименьших значащих бит происходит не обнуление областей встраивания, а их преобразование.

Используя результаты теоретических исследований, полученные в работе [1], рассмотрим практическое применение двухкомпонентного контейнера при встраивании информации в растровые изображения без сжатия.

Шакурский Максим Викторович, доцент кафедры "Теоретическая и общая электротехника".
E-mail: M.Shakurskiy@gmail.com

Статья поступила в редакцию 27марта 2020 г.

Встраивание информации осуществляют в соответствии со следующей математической моделью [1]:

$$\begin{cases} y_1 = a_1 + b_1 u_1 + c_1 \xi; \\ y_2 = a_2 + b_2 u_2 + c_2 \xi, \end{cases} \quad (1)$$

где u_1 и u_2 — информативные сигналы, полученные из скрываемого информативного сигнала u;
ξ — маскирующий сигнал (сигнал контейнера).

Встраиваемые сигналы u_1 и u_2 формируют из сигнала сообщения с помощью коэффициента связи:

$$\begin{aligned} u_1 &= u; \\ u_2 &= K - u_1, \end{aligned} \quad (2)$$

где K — коэффициент связи.

Извлечение сообщения осуществляют с помощью выражения

$$u = u_1 = \frac{K b_2 c_1 - a_1 c_2 + a_2 c_1 - c_1 y_2 + c_2 y_1}{b_1 c_2 + b_2 c_1}. \quad (3)$$

Максимальная чувствительность системы к вариации ключевых коэффициентов (3) наблюдается вблизи точки разрыва:

$$b_1 c_2 + b_2 c_1 = \sigma \text{ при } \sigma \to 0, \quad (4)$$

где σ — величина отклонения от точки разрыва.

Имитационное моделирование

Рассмотрим встраивание компонент (1) в область наименьших значащих бит. Для этого сформируем блоки из четырех пикселей следующим образом: первые два пикселя блока содержат сигналы y_1 и y_2 компонент контейнера, а вторые два пикселя — сигналы y_3 и y_4, компенсирующие искажение статистических характеристик от встраивания сигналов y_1 и y_2. В данном случае для маскировки сигналов u_1 и u_2 сообщения используются псевдослучайный сигнал и последующее встраивание компонент y_1 и y_2 в область наименьших значащих бит.

В численном примере используем для встраивания битный узор (рис. 1).

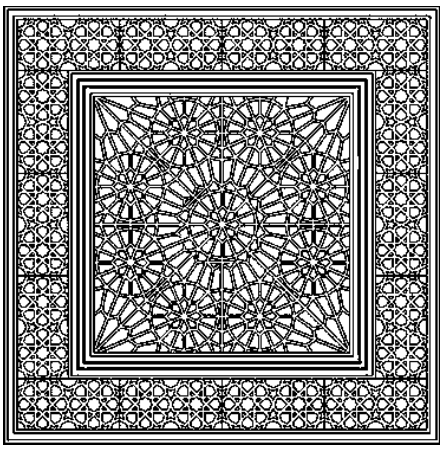


Рис. 1. Секретное сообщение — битный узор

В качестве контейнера используем изображение (рис. 2).

Рис. 2. Изображение контейнера

Младшие биты изображения контейнера представляют собой некоррелированный шум. На рис. 3 представлены битные изображения, соответствующие четырем младшим битам контейнера. Выполним встраивание компонент в три младших бита. Численное исследование выполним в среде Mathcad.

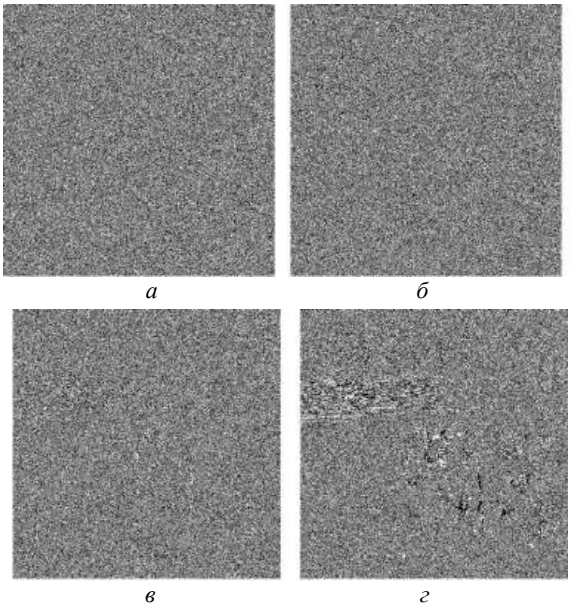


Рис. 3. Содержимое младших бит изображения контейнера по слоям: *а* — восьмой бит; *б* — седьмой бит; *в* — шестой бит; *г* — пятый бит

Сформируем маскирующий сигнал:

$$\mathrm{NoizeAmp} := 5$$

$$\xi_{\mathrm{row,\,col}} := \mathrm{round}\left(\mathrm{md}\left(\mathrm{NoizeAmp}\right)\right)$$

Зададимся значениями коэффициентов с учетом (4):

$$a1 := 1 \quad a2 := 4 \quad b1 := 1 \quad b2 := -2$$

$$c1 := 1 \quad \sigma := 0.01 \quad n := 1 \ldots 256$$

$$c2 := \frac{-b2 \cdot c1}{b1} = 2 \quad c2 := 1$$

Сформируем компоненты стеганографической системы:

$$y1_{\mathrm{row,\,col}} := a1 + b1 \cdot u1_{\mathrm{row,\,col}} + c1 \cdot \xi_{\mathrm{row,\,col}}$$

$$\max\left(y1\right) = 7 \quad \min\left(y1\right) = 1 \quad mu1 := \max\left(y1\right) = 7$$

$$y2_{\mathrm{row,\,col}} := a2 + b2 \cdot u2_{\mathrm{row,\,col}} + c2 \cdot \xi_{\mathrm{row,\,col}}$$

$$\max\left(y2\right) = 7 \quad \min\left(y2\right) = 0 \quad mu2 := \max\left(y2\right) = 7$$

$$\mathrm{Stego}_{\mathrm{row}\cdot 2-1,\,\mathrm{col}\cdot 2-1} := y1_{\mathrm{row,\,col}}$$

$$\mathrm{Stego}_{\mathrm{row}\cdot 2-1,\,\mathrm{col}\cdot 2-1} := y2_{\mathrm{row,\,col}}$$

Массив Stego представляет собой массив встраиваемых значений в область младших бит изображения. В результате маскировки встраиваемой битной последовательности псевдослучайным сигналом с равномерным распределением плотно-

сти вероятности (РПВ) сигналы y_1 и y_2 приобретают близкое к нормальному РПВ. Младшие биты пустого контейнера имеют равномерное РПВ. Для незаметности вложения применим метод компенсации РПВ двумя дополнительными значениями, y_3 и y_4, в области младших бит. Заметим, что данный пример не учитывает распределение старших бит, что ведет к заметной дивергенции Кульбака—Лейблера между заполненным и пустым контейнерами. Однако при стегоанализе рассматривают младшие биты. Выполним компенсацию РПВ в области младших бит:

$$YC := \text{imhist}(Cov, 256) \quad YC'_n := \frac{YC_n}{rw1 \cdot cl1 \cdot 4}$$

$$YC''_n := YC'_n - \frac{1}{8}$$

$$Y1 := \text{imhist}(y1, 256) \quad Y1'_n := \frac{Y1_n}{rw1 \cdot cl1}$$

$$Y1''_n := 0 \text{ on error } Y1''_{n-1} + \left(\frac{1}{8} - Y1'_n\right) + \frac{1}{8} + YC''_n \cdot 2$$

$$Y2 := \text{imhist}(y2, 256) \quad Y2'_n := \frac{Y2_n}{rw1 \cdot cl1}$$

$$Y2''_n := 0 \text{ on error } Y2''_{n-1} + \left(\frac{1}{8} - Y2'_n\right) + \frac{1}{8} + YC''_n \cdot 2$$

$$y3_{row,\,col} := \left| \begin{array}{l} i \leftarrow \text{md}(1) \\ 0 \quad \text{if } i \geq 0 \wedge i \leq Y1''_1 \\ 1 \quad \text{if } i > Y1''_1 \wedge i \leq Y1''_2 \\ 2 \quad \text{if } i > Y1''_2 \wedge i \leq Y1''_3 \\ 3 \quad \text{if } i > Y1''_3 \wedge i \leq Y1''_4 \\ 4 \quad \text{if } i > Y1''_4 \wedge i < Y1''_5 \\ 5 \quad \text{if } i \geq Y1''_5 \wedge i < Y1''_6 \\ 6 \quad \text{if } i \geq Y1''_6 \wedge i < Y1''_7 \\ 7 \quad \text{otherwise} \end{array} \right.$$

$$Stego_{row \cdot 2,\, col \cdot 2 - 1} := y3_{row,\, col}$$

$$y4_{row,\,col} := \left| \begin{array}{l} i \leftarrow \text{md}(1) \\ 0 \quad \text{if } i \geq 0 \wedge i \leq Y2''_1 \\ 1 \quad \text{if } i > Y2''_1 \wedge i \leq Y2''_2 \\ 2 \quad \text{if } i > Y2''_2 \wedge i \leq Y2''_3 \\ 3 \quad \text{if } i > Y2''_3 \wedge i < Y2''_4 \\ 4 \quad \text{if } i \geq Y2''_4 \wedge i < Y2''_5 \\ 5 \quad \text{if } i \geq Y2''_5 \wedge i < Y2''_6 \\ 6 \quad \text{if } i \geq Y2''_6 \wedge i < Y2''_7 \\ 7 \quad \text{otherwise} \end{array} \right.$$

$$Stego_{row \cdot 2,\, col \cdot 2 - 1} := y4_{row,\, col}$$

Результат компенсации РПВ младших бит приведен на рис. 4.

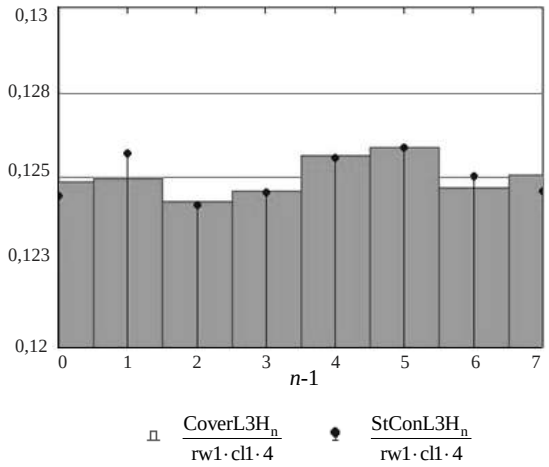


Рис. 4. Плотность распределения вероятности для трех младших бит исходного контейнера (серые столбцы) и заполненного контейнера (черные отсчеты)

Серыми столбцами показано РПВ пустого контейнера, черными отсчетами — заполненного. Дивергенция Кульбака—Лейблера для младших бит равна

$$DKL := \sum_{n=1}^{256} \left[\frac{CoverL3H_n}{(rw1 \cdot cl1 \cdot 4)} \cdot 0 \text{ on error } \log\left[\frac{\frac{CoverL3H_n}{(rw1 \cdot cl1 \cdot 4)}}{\frac{StConL3H_n}{(rw1 \cdot cl1 \cdot 4)}}, 2 \right] \right]$$

$$DKL := 6{,}533 \times 10^{-6}$$

На рис. 5 приведено изображение на основе трех младших бит заполненного контейнера (для повышения яркости добавлена постоянная составляющая). В нем не просматривается встроенное сообщение.

Рис. 5. Изображение, содержащее три бита встраиваемой в контейнер информации

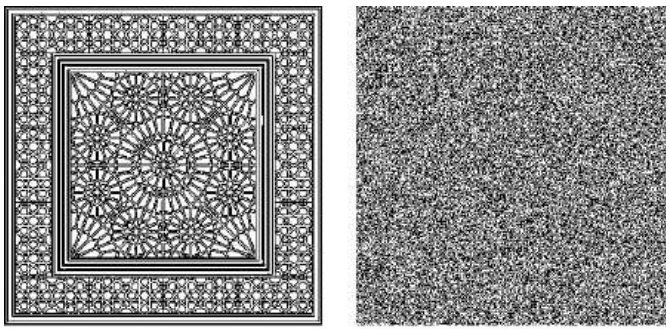
На рис. 6 приведено изображение заполненного контейнера.

Рис. 6. Заполненный контейнер

Извлечение сообщения происходит путем выделения трех младших бит заполненного контейнера, выделения компонент и применения к ним выражения (3):

$$u1'_{row,\,col} := \frac{\left(\begin{array}{c} K \cdot b2 \cdot c1 - a1 \cdot c2 + a2 \cdot c1 - \\ -c1 \cdot y2dec_{row,\,col} + c2 \cdot y1dec_{row,\,col} \end{array}\right)}{b1 \cdot c2 + b2 \cdot c1}$$

На рис. 7 приведены результаты извлечения скрытой информации без ошибок в ключевых коэффициентах и с минимальной ошибкой в значении одного коэффициента. Видно, что наличие ошибки в значении коэффициентов не позволяет обнаружить скрытое сообщение.



а *б*

Рис. 7. Извлеченное сообщение:
а — без ошибок в значениях коэффициентов; *б* — с ошибкой в значении ключевого коэффициента

Заключение

В результате проведенного исследования предложен алгоритм встраивания двухкомпонентного контейнера в область наименьших значащих бит изображения. В роли маскирующего сигнала при формировании компонент контейнера можно использовать как псевдослучайный сигнал, так и значения младших бит контейнера. Предложенный алгоритм опирается на исследования, относящиеся к методу наименьших значащих бит, который используют в однокомпонентных контейнерах. Эффективность использования двухкомпонентного контейнера определяется возможностью маскировать сообщение с помощью перемешивания сигналов сообщения и контейнера и извлекать его без знания контейнера.

Литература

1. *Шакурский М. В.* Двухкомпонентная стеганографическая система на основе суммы линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов // Вопросы защиты информации. 2020. № 1 (128). С. 10—13.

2. *Шакурский М. В., Козловский В. Н.* Выбор ключа в инвариантных двухкомпонентных стеганографических системах, использующих мультипликативный алгоритм связи встраиваемых сигналов. // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4 (123). С. 3—9.

3. *Шакурский М. В.* Свойства инвариантных двухкомпонентных стеганографических систем, использующих аддитивный алгоритм связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 4 (123). С. 3—9.

4. *Шакурский М. В.* Математические модели двухкомпонентных инвариантных стеганографических систем, использующих различные алгоритмы связи встраиваемых сигналов // Вопросы защиты информации. 2018. № 2 (121). С. 8—13.

5. *Шакурский М. В., Шакурский В. К.* Устройство сокрытия информации. Патент 2546307 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. № 10.

6. *Шакурский М. В., Шакурский В. К.* Способ скрытой передачи информации. Патент 2546306 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 10.06.2014. Опубл. 10.04.2015. Бюл. № 10.

7. *Шакурский М. В.* Устройство сокрытия информации. Патент 167074 РФ, МПК H04L 9/00, H04K 3/00. Заявл. 28.01.2016. Опубл. 20.12.2016. Бюл. № 35.

8. *Шакурский В. К., Шакурский М. В.* Сжимающие отображения в инвариантных преобразователях и системах стеганографии. — Самара: Изд-во СНЦ РАН, 2014.

9. *Шакурский М. В.* Формирование контейнера для стеганографической системы на основе сжимающих отображений // Радиотехника. 2015. № 2.С. 134—139.

10. *Шакурский М. В., Шакурский В. К.* Стеганографическая система на основе сжимающих отображений // Вопросы защиты информации. 2015. № 2. С. 74—78.

A method of embedding information in the low bits of raster images without compression, using a two-component container

M. V. Shakurskiy
Samara State Technical University, Samara, Russia

The article discusses the method of embedding information in the lower bits of a raster image without compression with preliminary masking of the message with a random signal. The message is masked using an information hiding algorithm based on the sum of the linear functions of two signals, using the additive form of constrain of embedded signals.

Keywords: two-component steganographic system, invariance to masking signal, steganographic container, key coefficient, raster image, least significant bit method.

Biography — 10 references. *Received Match 27, 2020*

УДК 681.3.06

Новое о шифре Уитстона

А. Б. Симон
ПАО «Уралмашзавод», Екатеринбург, Россия

Описан шифр симметричного блочного шифрования с размером блока 128 бит, в котором не используются такие общепринятые понятия, как операция XOR, раундовые ключи, сеть Фейстеля, SP-сеть, таблицы замен. Показан новый подход к использованию идей шифра Уитстона.

Ключевые слова: текст, шифртекст, массив, пара, байт, бит

Автор много экспериментировал с шифром двойного квадрата Уитстона [1]. Вначале вместо биграмм этим шифром он стал шифровать трех- и четырехграммы, затем — максимально избыточные тексты вида "ааа…ааа" [2]. Потом два квадрата Уитстона превратились в два массива 16×16, заполненные байтовым алфавитом, и ими стали шифроваться 128-битные блоки вида "000…000" и "000…001". В режиме счетчика было зашифровано 256 блоков только из нулевых бит. Блоки шифровали за 8 раундов. В другом "авторском" режиме было зашифровано 120 блоков из нулевых бит и для проверки лавинного эффекта [3] — в этом же режиме и эти же блоки, но с единичным последним битом. Здесь блоки шифровались за 6 раундов. Автор данной работы убедился в том, что при шифровании с использованием идей Уитстона можно обойтись без таких понятий, как операция XOR, раундовые ключи, сеть Фейстеля, SP-сеть, таблицы замен [4]. О рабочих качествах описанного шифра говорить рано, но сам подход к задаче может оказаться интересным.

Алгоритм шифрования

Описан симметричный шифр блочного шифрования с размером блока 128 бит. В этом шифре использована побайтовая замена текста на шифртекст. Это выполнено с помощью двух массивов размером 16×16, в каждом из которых в случайном порядке записан байтовый алфавит 00, 01, …, fe, ff.

В качестве примера опишем один раунд шифрования. В нашем случае правила шифрования не зависят от размера массивов, поэтому используем массивы A_0 и A_4 размером 4×4 (рисунок). Также для примера в массивы в случайном порядке вместо байтов запишем полубайты 0, 1, …, e, f. Поочередным сдвигом массива A_0 относительно массива A_4 на одну строку вверх получим четыре пары массивов:

- пара 0 — A_0 и A_4;
- пара 1 — A_1 и A_4 (массив A_1 — это массив A_0, сдвинутый на одну строку вверх);
- пара 2 — A_2 и A_4 (массив A_2 — это массив A_0, сдвинутый на две строки вверх);
- пара 3 — A_3 и A_4 (массив A_3 — это массив A_0, сдвинутый на три строки вверх).

При необходимости массивы A_1, A_2, A_3 можно заменить массивом A_0 с коррекцией вертикальной координаты.

A_0

8	4	d	f
c	2	e	b
7	a	3	0
6	1	9	5

A_1

c	2	e	b
7	a	3	0
6	1	9	5
8	4	d	f

A_2

7	a	3	0
6	1	9	5
8	4	d	f
c	2	e	b

A_3

6	1	9	5
8	4	d	f
c	2	e	b
7	a	3	0

A_4

e	1	3	8
4	0	c	5
7	2	9	d
b	f	6	a

Шифрующие массивы

Установим правила замены полубайтов.

- Пара массивов выполняет замену пары полубайтов.
- Каждая следующая пара полубайтов сдвигается относительно предыдущей на один полубайт вправо (подчеркнутые полубайты в табл. 1).
- Заменяющий полубайт берут из той же таблицы, в которой находится заменяемый. Например, если полубайт находится в таблице A_0, замену ему надо брать тоже в таблице A_0.
- Левый заменяемый полубайт находят в левом массиве, правый — в правом (исключение составляет последнее в списке правило замены). Эти полубайты считают углами воображаемого прямоугольника и в других углах берут замену. Например, полубайт 2 из строки 2 табл. 1 находим в массиве A_1, полубайт 0 — в массиве A_4, считаем эти полубайты углами прямоугольника и в других углах берем замену a1.
- Если заменяемые полубайты находятся в одной строке, левый заменяющий полубайт заимствует координаты правого заменяемого полубай-

Симон Адольф Брунович, ведущий конструктор.
E-mail: simonadol@yandex.ru

Статья поступила в редакцию 3 мая 2020 г.

та, а правый заменяющий полубайт — левого заменяемого полубайта. Например, полубайты 62 будут заменены парой A_1—A_4 на 17.

- Если у заменяемых полубайтов одинаковые координаты, замены не производят (см., например, строку 3 табл. 1).
- В паре "последний полубайт блока — первый полубайт блока" последний полубайт блока заменяют в левом массиве, первый — в правом. Например, в строке 4 табл. 1 полубайт 0 заменяем на 7 в массиве A_3, а полубайт b — на a в массиве A_4.

Таблица 1

Один раунд шифрования

Открытый текст 0000. Вариант шифрования 0123. Заменяемые и заменяющие полубайты подчеркнуты. За один раунд текст 0000 заменен на шифртекст aa17					
Строка	№ пары массивов		Шифрующие массивы	Текст	
1	Вариант шифрования	0	A_0—A_4	До замены	0 0 0 0
				После замены	b 2 0 0
2		1	A_1—A_4	До замены	b 2 0 0
				После замены	b a 1 0
3		2	A_2—A_4	До замены	b a 1 0
				После замены	b a 1 0
4		3	A_3—A_4	До замены	b a 1 0
				После замены	a a 1 7

Зашифруем блок из четырех нулевых полубайтов 0000. В данном шифре для каждого блока задают свой, индивидуальный вариант шифрования в виде перестановки из пар массивов. Для нашего блока зададим вариант шифрования 0123. Это значит, что в позиции первого полубайта блока для замены текста будет использована пара 0, в позиции второго полубайта — пара 1, в позиции третьего — пара 2, в позиции четвертого — пара 3. Один раунд шифрования показан в табл. 1. Дополнительные раунды выполняют в таком же порядке без смены варианта шифрования.

Все изложенное справедливо и при шифровании с использованием массивов размером 16×16 со следующими уточнениями:

- будет задействовано не четыре, а шестнадцать пар массивов размером 16×16;
- в ячейки массивов будут записаны байты, и заменяться по описанным правилам будут не полубайты, а байты.

Общее описание шифра

Размер ключа шифра 256 бит. Перед шифрованием выполняют расширение ключа до двух массивов размером 16×16. В каждый массив в случайном порядке записывают байтовый алфавит 00, 01, …, fe, ff. Возможен прямой ввод расширенного ключа.

Шифрование обеспечивают 16 пар массивов: 0, 1, …, e, f. Массивы, полученные при расширении ключа, принимают за пару 0. Пару 1 создают сдвигом массивов пары 0 относительно друг друга на 1 строку. Пару 2 создают сдвигом массивов на 2 строки и т. д. Фактически при шифровании используют только пару 0 и параметр Δ, учитывающий сдвиг массивов, где Δ = 0, 1, …, e, f. Каждому блоку задают свой, индивидуальный вариант шифрования в виде перестановки из 16 пар массивов. Пары используют побайтно. Например, вариант шифрования 4d5980cfe6231ab7 использует в позиции первого байта блока пару 4, в позиции второго байта — пару d, в позиции третьего — пару 5 и т. д. В одном цикле можно задать $16! \approx 2^{44}$ вариантов шифрования. Вложенными циклами можно задать $16!^c$ вариантов, где c = 1, 2, 3 — число использованных циклов. Ход шифрования по раундам показан в табл. 2.

Таблица 2

Ход шифрования по раундам

Вариант шифрования			0 1 2 3 4 5 6 7 8 9 a b c d e f
Открытый текст			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Шифртекст	Раунд	1	80 63 82 81 a0 6f 9e 5d 7c 4b 5a 49 c8 47 46 87
		2	67 53 54 9a 5b bf 3b 94 15 c4 d0 31 80 06 73 f5
		3	ad eb 2e f5 80 3a 5f 41 26 f0 9a e5 24 bf f5 09
		4	0a 3c 51 ed f0 ae 29 c0 a6 37 35 6d e8 e6 74 ce
		5	02 ab b5 2b b2 94 e0 1b b4 9e b3 37 ba c8 3c b7
		6	5b eb 02 e3 51 70 b5 9a 9c a9 a2 44 40 cd 6a a5
Изменим значение последнего бита: 0 → 1. Зашифруем текст: 00…01			
Вариант шифрования			0 1 2 3 4 5 6 7 8 9 a b c d e f
Открытый текст			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
Шифртекст	Раунд	1	d3 63 82 81 a0 6f 9e 5d 7c 4b 5a 49 c8 47 4a 67
		2	99 43 a4 ca 9b cf bb a4 f4 24 50 41 60 28 80 7f
		3	57 c6 62 25 11 2c 61 14 10 eb e5 76 4f 83 0d 2b
		4	fe e5 de 74 8a 2f fa 6a 38 16 7f f4 85 f4 76 fd
		5	3c fe 03 bf 6e 51 3a 81 a3 32 21 b3 af fc 0c 85
		6	43 52 42 1d a8 ef a0 40 d0 84 28 62 46 d0 20 a8
Поменяем местами пары 0 и f. Зашифруем текст: 00…00			
Вариант шифрования			f 1 2 3 4 5 6 7 8 9 a b c d e 0
Открытый текст			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Шифртекст	Раунд	1	b3 43 62 51 80 8f 7e 1d dc ab ea 59 88 17 46 18
		2	07 e5 9a dd 89 3a e0 a6 38 1d 82 86 ee 36 33 31
		3	96 3f 10 d9 20 a0 bc b1 be 8b 54 d9 2a 71 26 e4
		4	40 e0 80 e0 29 46 f1 f9 97 13 18 38 04 3a 97 42
		5	52 af 03 a6 0f 86 48 61 6d c8 0e 2b 78 9b 58 93
		6	0c 52 c0 68 fa 70 ce f6 a4 3c da e1 1c 86 5d e3

Заполнение массивов при расширении ключа производят из служебного шифртекста. Служебный шифртекст создают шифрованием открытого текста, состоящего из 16 ключей шифрования, записанных друг за другом. Общий размер этого текста 512 байт или 32 блока. Каждому блоку задают свой, индивидуальный вариант шифрования. Блок шифруют за 6 раундов. Шифрование выполняют исходным расширенным ключом из двух массивов 16×16, записанным в исходном коде программы. Из служебного шифртекста байты поочередно переписывают в один из массивов расширяемого ключа. При этом исключен повтор байтов: в массив пропускают только разные по величине байты. Если служебный шифртекст полностью использован, а массив не заполнен до конца, шифртекст обновляют еще одним раундом шифрования всех блоков и затем продолжают заполнение. После заполнения первого массива шифртекс вновь обновляют и в той же последовательности заполняют второй массив. После каждого обновления очередность байтов в служебном шифртексте меняется. Это обеспечивает разное, достаточно случайное положение байтов в первом и втором массивах.

В качестве синхропосылки можно использовать вариант шифрования первого блока. Возможны синхропосылки для расширения ключа и для шифрования текста. Разным синхропосылкам будут соответствовать разные расширенные ключи и разные шифртексты (табл. 3).

Расширение ключа и шифрование текста выполняют одними и теми же операциями. Рекомендуемое число раундов шифрования представлено в табл. 4.

Расшифровка отлична от зашифровки только обратным порядком выполнения операций.

Таблица 3

Примеры синхропосылок

Число циклов *c*	Синхропосылка	Количество
1	4d5980cfe6231ab7	2^{44}
2	4d5980cfe6231ab7 0123456789abcdef	2^{88}
3	4d5980cfe6231ab7 0123456789abcdef 23ab01c456789def	2^{132}

Таблица 4

Рекомендуемое число раундов шифрования

Режим	Число циклов *c*	Число вариантов шифрования	Рекомендуемое число раундов
Режим задания вариантов шифрования	1	2^{44}	Не менее 6
	2	2^{88}	Не менее 7
	3	2^{132}	Не менее 8
Режим счетчика	Счетчик может выдать 2^{128} значений		Не менее 8

Пробное тестирование шифра

Результаты тестирования шифра даны в табл. 5—7, где все блоки зашифрованы на одном ключе независимо друг от друга. При тестировании в одном массиве пары 0 байты были размещены хаотично, в другом — по возрастанию: 00, 01, …, fe, ff.

Шифр в режиме независимого шифрования блоков одинаковые тексты заменяет на разные шифртексты. Возможно параллельное шифрование нескольких блоков.

В табл. 5 и 6 показано влияние на результат шифрования:

- изменения значения одного бита;
- перестановок пар массивов.

Таблица 5

Зашифровка блоков 00…00

Варианты шифрования получены перестановкой пар 0, 1, 2, 3, 4. Зашифровано 40 блоков с одинаковым открытым текстом 00000000000000000000000000000000. Шесть раундов шифрования		
№	Вариант шифрования	Шифртекст
1	fedcba9876543210	a702d53d9161887dd5ef4ad89f09c1fc
2	fedcba9876543201	79afb431f1d572182df65494203364ce
3	fedcba9876543120	97d55d65201d7b0c8882d1255ee81812
4	fedcba9876543102	b5d38ddb49c04ead2bc529ef604d7d9f
5	fedcba9876543021	c03d56ed3805c8996196a9286abbe964
6	fedcba9876543012	301edc29221f282bdf38dbe043ed4549
7	fedcba9876542310	6cf7a59736df6c8d56f109c69b9899d7
8	fedcba9876542301	bb4e3a3af499129b6c9f4c0e1f6b8540
9	fedcba9876542130	b349000e503b77b941712b80d8cbcf2a
10	fedcba9876542103	72c702a80e44d1ff6d62c75a61c24ac1
11	fedcba9876542031	6ed529376d99bdf833d51f9db0f3c4b9
12	fedcba9876542013	200da0ac7721cfc16d84216e1c75dfbe
13	fedcba9876541320	367fe7fc60527d2d6fd7556c822e6e57
14	fedcba9876541302	35d5f71640ca9e5a3841cd2bb2dbfaac
15	fedcba9876541230	0d606ae6c37b6ccf5d2885aea36d7c0c
16	fedcba9876541203	0cadffd1c843846441b65bb343883114
17	fedcba9876541032	f684c1ced56cffc5b090b511dd000c97
18	fedcba9876541023	be026948aec73344908157c20525bc97
19	fedcba9876540321	ef84d9b34ee9dd7d48e671582fda54c8
20	fedcba9876540312	184c88c2e5501a51e66c5a2e435502e2
21	fedcba9876540231	442d40e431030fdb73eb7cc627213271
22	fedcba9876540213	539530cd9de770838b4170dd1eb162ff
23	fedcba9876540132	b2d0fe7216c8357df93904276c513eed
24	fedcba9876540123	0d901cd1c7ba1af0838f167e4d9e9a7e
25	fedcba9876534210	d1e2c3794cebc93a3e62713b12cbe3f6
26	fedcba9876534201	c6855edededb26903c0cbf00c79dc6ce
27	fedcba9876534120	3445e8f9a9ce8eb5b60d8674cde08c14
28	fedcba9876534102	22e2e0460e8359027240de25c36a3411
29	fedcba9876534021	22348063fb2a1ae0d646dd1b5fd86d25
30	fedcba9876534012	5abb0f0bb7bb3f6f5d950335f7a7c0bb
31	fedcba9876532410	065a99320f4914a05b26f7c0e6b1d8a5
32	fedcba9876532401	4bf646294e042b612eef17fd068856a5
33	fedcba9876532140	5d6ac1eca5a06f31785b73a6127c7346
34	fedcba9876532104	46cbdcbd0fa07cbdd5352e3e574ef8fb
35	fedcba9876532041	6d382adcb94b36d8a1ea1ad171b092fb
36	fedcba9876532014	6127913b4a0dc6fe3e7c700d3e5102f4
37	fedcba9876531420	9b21a546906ace54ae295e52fb8c24f4
38	fedcba9876531402	0a3c07d93c8893e0ef998fe81a70b8ae
39	fedcba9876531240	92d3cf8079ab1f0cd2b87a865b6c50a5
40	fedcba9876531204	e4e814d50c5494d14396c14aad277630

Таблица 6

Зашифровка блоков 00…01

Варианты шифрования получены перестановкой пар 0, 1, 2, 3, 4. Зашифровано 40 блоков с одинаковым открытым текстом 00000000000000000000000000000001. Шесть раундов шифрования		
№	Вариант шифрования	Шифртекст
1	fedcba9876543210	358cfe7ac271f0fd6b9f11509014037a
2	fedcba9876543201	4739854bb797297f6e729ff14a9e03f0
3	fedcba9876543120	9dd0b80dedaf06f4b741ab281d86f2b3
4	fedcba9876543102	9d02e5bf9c9787166549f6dfeee0e4a6
5	fedcba9876543021	b3f195057ac99edbf051731544a921ad
6	fedcba9876543012	c050a0c65734731e67625d5a0034dafc
7	fedcba9876542310	f786f8f8fa014823070e230eb25f379c
8	fedcba9876542301	b56026afcd52a6b05ec2098cd02506a4
9	fedcba9876542130	a648a46111370a6c6cb0c3b8fe389210
10	fedcba9876542103	38ef2988f1f3f466dd792feadafc0a5a
11	fedcba9876542031	4a84ab095b7a9f5efd1457c27eb40244
12	fedcba9876542013	8b3d352261584205e6c0567606ab5788
13	fedcba9876541320	a8fdcd34876fc384dc1f2c44d20abcbe
14	fedcba9876541302	d5106dca3e7abadb630b579a83c2dd74
15	fedcba9876541230	e4e5f49d90cb1e4861c6a5cbec745d84
16	fedcba9876541203	9380923887103b6edd0e54c250a98b4b
17	fedcba9876541032	009dfb510d8b63f5ecb67d7ce1fbaa00
18	fedcba9876541023	b2b8022aa113f2ed89d39ea840dae011
19	fedcba9876540321	47c501b1c5d05102be89d3a56e60ae7a
20	fedcba9876540312	edaa29ad609baa873ea3f6ea5627076a
21	fedcba9876540231	3922939c3d2de25baf9b66fcebc189f8
22	fedcba9876540213	f30e4401ca6f68dcb0a8bfac58d9e01e
23	fedcba9876540132	9b16a2e1ac41008eb91062930772c833
24	fedcba9876540123	d6529b1b2da0d4e06eb5efb24d977058
25	fedcba9876534210	03f37798b6e82d819c69fb6a274f2d75
26	fedcba9876534201	b819e74ac27e6cf937a61cc9a034f2f7
27	fedcba9876534120	faffbd5d2b96ac51c34af1f82642939e
28	fedcba9876534102	211731a964ccd3206e77af799e187edc
29	fedcba9876534021	c10cab6f12b396813c1e95cea55531fc
30	fedcba9876534012	47a44b114a822dca5c5af32df11bf5cd
31	fedcba9876532410	dff3fb9d8a195c93f7dfc9d1e7678a52
32	fedcba9876532401	bb0df79d29de351584adc2248bf1b97d
33	fedcba9876532140	0de7c8999f93b4a641dc227b55e70934
34	fedcba9876532104	f373338ae610f31eaebc4b4b253b6348
35	fedcba9876532041	fb08772f6aa65a42185feb7d5f2e67f8
36	fedcba9876532014	d3ec578d7ff37e0b173b37e904af3b25
37	fedcba9876531420	4306257aa119528840b6bdf414196008
38	fedcba9876531402	8449a2f811531916cb1709743804abdb
39	fedcba9876531240	14882ffe2e0984404f998dfa264ef892
40	fedcba9876531204	c73c51d3de5c157145b56b54334ec2db

В табл. 7 даны результаты тестирования шифра в режиме счетчика, когда шифруют сумму открытого текста блока и значения счетчика.

В этом режиме при шифровании всех блоков используют одну и ту же перестановку пар массивов.

В режиме счетчика в качестве синхропосылок можно использовать:

- произвольное стартовое значение счетчика (2^{128} вариантов);
- одну из перестановок пар массивов (2^{44} вариантов).

В режиме счетчика при многократном шифровании одного и того же текста размером 128 бит шифр может выдать 2^{128} разных шифртекстов.

Таблица 7

Режим счетчика

У всех 80 блоков открытый текст 00000000000000000000000000000000 и вариант шифрования 0123456789abcdef. Восемь раундов шифрования. Шифруется сумма открытого текста блока и значения счетчика СЧ			
СЧ	Шифртекст	СЧ	Шифртекст
00	fc9b51f9d6077a1a3ba7656f0ff3c1b5	28	bedcc51bf8a4afea76e88a20591e729b
01	7945949a8af8447267f26c987d765ffb	29	9db4e73a4a899dbf98e1c2075a5bc3e3
02	87f90790a2a50c6d4a4c76e4f0d6a187	2a	05b87bf6df09f57a17b92740a792a6f6
03	7b5742e7d02dcb8172f5f2fef7b53e25	2b	0b7989ed3f664f409ed0775074130473
04	b3fe38d6769d4e0c4bc67c9c94f992a9	2c	ad84e06f4665298c2b44100fa92143b8
05	4fc93c38b8ab0e4e91a10295838c15ff	2d	2474d150f19389ffd0d24512d03fb003
06	4084b8119747439e0f2545ad53b68277	2e	5089685521add7c08629cf0d61b4fd96
07	0b3595356d326974e5a591571e5aa863	2f	52cd0161e76e50799f1225efa6aecda0
08	e24dadb4543e8dc0cb1214bb6752c6f2	30	c4770bdacbd7bf56489b4cae9dbc9981
09	b0d2e9d1278ea0593fb2d3525a09c50a	31	8a6fb8dc0988c283de5022f66c01c7f0
0a	d71ffc6f41e6d20cfabb36940c92df4d	32	74b87be63f59351a1774d090ac233f28
0b	6b0cb7d8c025b85141d3ad30c63b036a	33	81455fd30f377ac60695b194c23dc948
0c	41c942ec0edaf8d42c79532929e54a9f	34	b44cd6794b40a1267b795d345f5d2e17
0d	7ceb1f2df5b328748cf9e5628bdd3882	35	35bbc9e6c924ffade75aa8b171a20b76
0e	6e56a96eb076d1a3bc166a7a686b72b6	36	601ad72c47f030c3e0b2ad5cc3704b17
0f	a8d5f0033ae132b5d6f81a33f4aa1ecb	37	ebfb7c5b396c723641a1ea69e0acbb48
10	1495f1944e79138234290a8a85f65068	38	be4652f6f538264a25139843f48c3f57
11	85594c2040cf2f0570c1a70264914020	39	344e6499311514e1a49ab9cc15f1fb3d
12	595387c9f705fc1f225d215f1a01e582	3a	4ac1eae770fd8b8192fc4621156011dc
13	6a4348e76c08c622c5403a3686391337	3b	81b1df060164f5ca89285b63e7764b89
14	0262da78e6b11a09354215fdb929988f	3c	b8eb027cb8ff3278cc839f39ecd8a860
15	bdbb9b0c880ff8540cec54233eacf014	3d	8cd1e230fa1fbdfcfb643eb2deddd6c9
16	ad43508a6dedf378ed73e951cd6ac5dd	3e	f55ec61780aab67a2489a0fab3da9237
17	8084715fbbf0d8f4b00279dffaf2d52a	3f	20ebb999129e953f1a1f5a41462a92df
18	f4ef9644805bdedee7aaffaf8e01d423	40	fd87dbfa8e958f0b3159bd786fde8251
19	1bd2ac062675b58bf76794c1f5466f91	41	64e96bb2a4be73af8cd2c10fffefa2f8
1a	12b515aa1fe26478389726a3848ead2c	42	2b7f3b5b2e80cc6a0ebeb928e4f2cb81
1b	1e7d1a1c94e1825db3e9bf5384f161d8	43	df2ef2de165f86688c531f2db19a6a97
1c	b3df9b45f970d39eeccf0cc668b9e135	44	f07b9d6dc3fa7f17d38c993710249313
1d	77178c71f104e28d029af67b61f6cbc1	45	09cdff093139ecb5f8cfd2efd4e76aeb
1e	f8cb4f5542ea3a69bfb2e982d7963960	46	b986e44f573dbc7d6a53c8e80cc0a806
1f	21bac131772e6039bf62b077b7249a70	47	0e645290d34c0e0c95d87e5dce4c853a
20	899bc4b794b048c47cf948a3b92f95a9	48	7e1bd84791e57a3e6565a4bb91dcec2c
21	605af6571c661eae35edf43c9f1db269	49	57e732bc438771ccb5cdc9afd1beb152
22	1b73daa2db6a0dad5bffc75597fc732e	4a	a65fedbaa5580716934e8de735dc19d3
23	7d0fddda50d2657e5741046fd34d951a	4b	ad211220fab0148b3ce99a4e27bea28d
24	7b743d2666db568b3cda554959cb4434	4c	d0a16ab1bb8e0cfa17b7557d2ff7069c
25	533afeaeb2bd510a5f31a776299a430f	4d	c755c736b2199e7ed5663a4c0e567ff0
26	57d1401f3518659a938203438d074478	4e	ef3b928ab80e6034ecddd441c54e5646
27	75afbcf5db3f7598f897ddcb6d96f107	4f	c358021750ac1c7fb891285793eb70eb

Дополнительные опции

Могут быть следующие дополнительные опции:

- допустимы блоки размером от 64 до 128 бит с шагом 8 бит (короткие блоки шифруют за меньшее число раундов; например, блок размером 64 бит шифруют за 4 раунда);
- допустимы ключи размером от 128 до 512 бит с шагом 8 бит;
- возможен прямой ввод расширенного ключа.

Заключение

Показана возможность создания шифра симметричного блочного шифрования без использования таких общепринятых понятий, как операция XOR, раундовые ключи, сеть Фейстеля, SP-сеть, таблицы замен. По-новому использованы идеи Уитстона. Необходимы доказательства быстродействия и криптостойкости шифра.

Литература

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В*. Основы криптографии: учеб. пособ. Изд. 2-е, испр. и доп. — М.: Гелиос АРВ, 2002. С. 32.
2. *Шеннон К*. Работы по теории информации и кибернетике / Пер. Писаренко В. Ф. — М.: ИЛ, 1963. С. 333—369.
3. Мат. III межд. науч.-практ. конф. "Актуальные проблемы безопасности информационных технологий" / под общ. ред. Жданова О. Н., Золотарева В. В. — Красноярск: Сиб. гос. аэрокосмич. ун-т, 2009.
4. *Панасенко С. П.* Алгоритмы шифрования: спец. справочник. — СПб.: БХВ-Петербург, 2009.

New about the Wheatstone cipher

A. B. Simon
JSC "Uralmashplant", Ekaterinburg, Russia

The article describes a symmetric block encryption cipher with a block size of 128 bits, which does not use such common concepts as the XOR operation, round keys, Feistel network, SP-network, and substitution tables. A new approach to using the ideas of the Wheatstone cipher is shown.

Keywords: text, ciphertext, array, pair, byte, bit.

Bibliography — 4 references. *Received May 3, 2020*

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056.52

Инструменты и средства для мониторинга состояния периферийных устройств

М. В. Пахомов
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

Изучены инструменты и средства для мониторинга состояния периферийных устройств сотрудников больших компаний. Установлена классификация типов периферийных устройств в соответствии с их назначением. Описаны существующие решения для контроля интерфейсов ЭВМ: встроенные в операционную систему (ОС) опции и программные комплексы, работающие в ОС и до ее загрузки. Показаны подходы, реализованные в этих инструментах. Получен перечень наиболее известных продуктов для контроля периферии. В этом перечне содержится информация о списке устройств периферии и интерфейсов ЭВМ, которые может контролировать конкретное средство защиты информации (СЗИ).

Ключевые слова: периферия, USB, СЗИ, DLP, контроль интерфейсов, мониторинг периферийных устройств.

Во многих сферах деятельности человека важной задачей является контроль со стороны управляющего персонала за использованием сотрудниками периферийных устройств в рабочее время, особенно в больших компаниях, когда речь заходит о сотнях и тысячах единиц вычислительной техники и значительном числе рабочего персонала, так как наличие только организационных мер неэффективно [1]. В подобных случаях необходимо обезопасить средства вычислительной техники от вредоносного программного обеспечения (ПО), сохранить конфиденциальность данных на устройстве и избежать утечки информации, правильно разграничить привилегии между сотрудниками и корректно управлять доступом к периферии [2].

Цель данной работы — составление перечня инструментов и подходов контроля подключения периферийных устройств к ЭВМ.

Основным объектом контроля является использование USB-флеш-накопителей, так как благодаря таким им свойствам, как дешевизна, компактность, доступность, легкость в эксплуатации, их используют повсеместно. При этом пользователи ЭВМ относятся к ним легкомысленно. Флеш-накопители достаточно легко теряют, заражают вирусами, их используют как на рабочей ЭВМ, так и на персональной, причем для них не ограничен перенос информации, из-за чего возрастает риск утечки. Также нельзя забывать, что конфиденциальность информации может быть нарушена с помощью Android/iOS-устройств. Информация может быть транслирована на сканеры/принтеры либо передана на такие альтернативные запоминающие устройства, как смарт-карты, диски и т. п.

Чтобы избежать утечек информации, используют различные средства защиты информации от несанкционированного доступа (СЗИ НСД). Существует множество таких решений, однако каждое из них имеет свою специфику по работе с периферией, определенный список контролируемых внешних устройств и параметров, по которым можно производить мониторинг подключений к ЭВМ. Из-за этого возникает неопределенность в решении вопроса о том, какие средства на самом деле способны устранить возможность утечки конфиденциальной информации через периферию, а какие лишь усложняют атакующему задачу нахождения нужного внешнего устройства и порта.

Автором составлен перечень периферийных устройств и интерфейсов ЭВМ, безопасность которых должны обеспечивать СЗИ и которые активно используются в компьютерных технологиях и весьма актуальны. Рассмотрены некоторые существующие решения для мониторинга и контроля периферии и различные подходы, реализованные в этих инструментах.

Пахомов Михаил Вадимович, студент.
E-mail: pahomov.mv@phystech.edu

Статья поступила в редакцию 14 апреля 2020 г.

Список использованных источников сформирован исходя из поставленных задач. Приведены источники, которые предоставляют основную информацию о периферийных устройствах, в том числе перечислена литература, в которой особое внимание уделено: USB; детальному рассмотрению наиболее известных и используемых интерфейсов и шин ЭВМ; существующим DLP-системам и СЗИ НСД. Представлены сравнительные характеристики средств защиты информации для ЭВМ.

Основные определения

"Периферийное устройство — это внешнее по отношению к центральному процессору и основной памяти дополнительное вспомогательное устройство, предназначенное для ввода и/или вывода информации в компьютер и расширяющее его функциональные возможности" [3, с. 63].

"Интерфейс (*interface*) — совокупность средств и правил, обеспечивающих взаимодействие устройств вычислительной машины или системы обработки информации и (или) программ" [3, с. 66].

Специализированные интерфейсы — интерфейсы, ориентированные на подключение устройств определенного узкого класса. В них используют сугубо специфические протоколы передачи информации [4].

Универсальные интерфейсы — интерфейсы, обладающие широким назначением, их протоколы обеспечивают доставку данных без привязки к специфике передаваемой информации [4].

Типы периферии

Для обеспечения комплексной защиты от утечек данных через внешние устройства по отношению к ЭВМ требуется составить список устройств периферии и интерфейсов ЭВМ, которые необходимо контролировать комплексами защиты.

В список интерфейсов входят [4—7]:

параллельный:

- LPT-порт (IEEE 1284);
- порт AGP;
- интерфейс ATA/ATAPI/SATA;
- интерфейс SCSI;
- шина PCMCIA;
- шина ISA;
- шина PCI/PCI-X;

последовательный:

- COM-порт (RS-232);
- интерфейс Thunderbolt;
- интерфейс SAS;
- шина USB;
- шина FireWire (IEEE 1394);
- шина PCI Express (PCIe, PCI-e).

Данный перечень интерфейсов не является исчерпывающим (или полным), а лишь затрагивает наиболее используемые интерфейсы, которые встречаются в большинстве ПЭВМ. Интерфейсы, не вошедшие в этот список, практически не применяют, и встретить их на рынке ПЭВМ непростая задача [7]. Также для этого перечня выбраны в основном шины и порты, которые используют преимущественно для передачи информации между ЭВМ и материальными носителями.

Среди указанных интерфейсов есть специализированные (LPT-порт, ATA, AGP, SAS, PCMCIA) и универсальные (COM-порт, SCSI, Thunderbolt, USB, FireWire, ISA, PCI). Поскольку специализированные интерфейсы ориентированы на узкий класс устройств, существует ограниченный список типов периферии для контроля со стороны СЗИ. В случае универсальных интерфейсов ситуация осложняется тем, что список возможных подключаемых устройств очень велик.

Следует отметить, что устройства, подключаемые к универсальным интерфейсам, могут быть разработаны сторонними разработчиками, и к взаимодействию с ними ЭВМ может быть изначально не пригодна. Для этого производитель может поставлять свой продукт в комплекте с ПО, содержащим драйвера для взаимосвязи с конкретной периферией. Универсальные интерфейсы используют повсеместно, поэтому становится трудно создать универсальную систему защиты ЭВМ от абсолютно всех возможных внешних устройств, т. е. нельзя априори предусмотреть работу СЗИ с любой периферией (возможно это реализуемо, но лишь на низком техническом уровне, на уровне управляемых сигналов на шинах устройства).

Следовательно, за исключением возможности мониторинга работы с определенными периферийными устройствами необходимо иметь контроль над всеми интерфейсами ЭВМ, т. е. администратор безопасности должен обладать возможностью полного отключения обмена информацией между ЭВМ и периферией через конкретный интерфейс. При этом в перечень контролируемых устройств должна входить наиболее используемая периферия [1, 8, 9]:

- оптические CD- и DVD-приводы, дисководы FDD;
- накопители FDD, CD-ROM, HDD, SSD, SD/MMC;
- встроенные сетевые карты, модемы;
- USB-флеш-накопители;

- фотокамеры, сотовые телефоны;
- локальные и сетевые принтеры.

Также стоит отметить, что в современных компьютерах универсальная шина USB заменила собой практически все другие виды портов для подключения периферийных устройств. На этот интерфейс перешли даже принтеры и сканеры, фото- и видеокамеры, клавиатуры и масса других периферийных устройств. При этом самыми используемыми USB-устройствами являются флешки и портативные жесткие диски. Поэтому на практике в 90 % случаев весь софт для контроля периферии используют непосредственно для контроля именно USB-портов [9].

Для подобного программного обеспечения недостаточно иметь лишь возможности активации/деактивации способности на передачу информации через USB со стороны администратора безопасности. Желательно, чтобы СЗИ позволяло разделять права доступа для разных пользователей ЭВМ, обладало административным интерфейсом для обновления и корректировки возможностей доступа пользователей к различным файлам на ЭВМ, предоставляло возможность контролировать передаваемые данные и (или) выполнять их теневое копирование.

Следует выделить несколько политик по защите информации, которые являются обязательными для всех программных изделий, имеющих целью контроль и мониторинг периферии [9—19]:

- идентификацию устройств по множеству параметров;
- разграничение доступа к устройствам на чтение, запись или полный запрет устройства;
- контроль (проверку на конфиденциальность вложенных данных) информации во время ее копирования, записи на устройства;
- копирование записываемых файлов в архив (теневая копия);
- запись информации об операции и файле в журнал событий.

Существующие решения

Инструменты для контроля периферии основаны на разных технических подходах и используют различные функции ЭВМ. Все существующие СЗИ ЭВМ разделяют на две группы по этапу, на котором они начинают свою инициализацию и работу. Это средства, работающие:

- после загрузки ОС;
- до загрузки ОС.

При этом работающие до загрузки операционной системы комплексы используют возможности BIOS (СЗИ НСД). Средства, работающие в ОС, могут быть:

- встроенными в ОС опциями;
- программными комплексами для ОС (DLP-системы).

Все такие средства имеют собственные возможности, различную сложность настройки и администрирования, разные степени полноты контроля над подконтрольными устройствами. Также следует отметить, что подобные средства защиты могут иметь дополнительные возможности и позволяют не только контролировать периферийные устройства, но и:

- идентифицировать и аутентифицировать пользователей ЭВМ;
- разграничивать доступ субъектов ЭВМ по некоторым мандатным таблицам к ресурсам ЭВМ;
- контролировать доступ к Internet и ресурсам в сети, реализовывать механизмы контентного мониторинга файлов;
- производить администрирование удаленному от ЭВМ администратору;
- вести систему отчетов и логов.

Встроенные в ОС опции. К данной группе решений можно отнести групповые политики в Windows, которыми обладает ОС и для которых необходима только правильная настройка. Они достаточно легки в конфигурировании в случае использования для индивидуального устройства. Возможности контроля у этого подхода имеют низкий уровень: разрешаются только полная блокировка/разрешение определенной внешней аппаратуры, которые могут выполняться лишь по малому набору параметров (в групповых политиках Windows возможно управление только с помощью ID-устройства) [20].

В результате этот подход практически не используют в силу малой базы возможностей.

Программные комплексы для ОС (DLP-системы). Эта группа средств содержит множество решений, которые очень удобны, легко настраиваемы, а также обладают обширным функционалом: мониторинг каналов сетевых коммуникаций и сетевых подключений, теневое копирование передаваемых данных, анализ содержимого файлов на предмет наличия в них конфиденциальных данных [1, 11—19].

К элементам данной категории относятся такие средства, как FileControl и Zecurion Zlock. Рассмотрим их более подробно. Эти программы разделяют администраторскую и пользовательскую части [1], поэтому можно дистанционно производить установку/удаление только пользовательской части на компьютеры корпоративной сети. Это

предоставляет возможность управления доступом к внешним устройствам и портам в соответствии с установленными администратором правилами через соответствующую административную консоль.

Данные средства также сохраняют в журнале событий всю информацию о времени подключения/отключения устройств и о том, какие файлы и когда были прочитаны и записаны на накопители или переданы на принтеры/сканеры. Это помогает найти нарушения при записи/чтении с внешних носителей информации. Более того, они предоставляют возможность теневого копирования ("программа без ведома пользователей сохраняет в отдельную папку на сервере все файлы, которые читались с внешних USB-дисков или записывались на них" [1]).

Однако такие средства имеют недостаток в виде более низкого уровня защиты по сравнению со средствами, работающими до загрузки ОС. Контроль над периферией, который предоставляет такие решения, зависит от клиентской части программы, расположенной в операционной системе рабочей ЭВМ. Поэтому если удастся, например, произвести загрузку с внешнего носителя в другой ОС, то никакого контроля и мониторинга над периферией не будет представлено, что может привести к утечке информации.

Продукты, работающие до загрузки ОС (СЗИ НСД). Данная группа средств значительно отличается от предыдущих, так как к ней относятся уже полноценные программно-аппаратные комплексы. Эти продукты нуждаются в физической охране ЭВМ и ее средств, в том числе в "проведении мероприятий по недопущению изъятия контроллера комплекса" [10].

К данной группе можно отнести программно-аппаратные комплексы средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) Аккорд и Secret Net от компаний ОКБ САПР и ИНФОРМЗАЩИТА соответственно. Это намного более сложные по архитектуре продукты в отличие от работающих в ОС средств, состоящие из множества компонентов [10]:

программные средства:

- драйверы;
- программы для работы с журналом и БД;
- система для контроля доступа;
- система для контроля целостности;

аппаратные средства:

- контроллер;
- устройство-съемник информации;
- персональный идентификатор.

Указанные средства могут обеспечить более высокую степень защиты в связи со своей аппаратно-независимой частью. Атака в виде загрузки с внешнего носителя против них неэффективна, так как процедуры идентификации, аутентификации и контроля целостности защищаемых файлов проходят до загрузки операционной системы. Уже до загрузки ОС с помощью процедуры авторизации определяют права пользователя ЭВМ на доступ к различным интерфейсам устройства и типам периферии.

Однако остается опасность физического изъятия контроллера комплекса из ЭВМ, из-за чего может возникнуть риск хищения информации с защищаемого устройства. Именно поэтому необходима физическая охрана ЭВМ и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса.

Подходы, реализованные в рассмотренных инструментах

Защита безопасности информации в таких инструментах основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам ЭВМ. При каждом программном или аппаратном прерывании, возникшем в случае пользовательского события, средства комплекса перехватывают это прерывание и в зависимости от соответствия полномочий субъекта доступа, установленных администратором, либо разрешают, либо запрещают обработку этих прерываний [10].

Это реально, так как взаимодействие программ, выполняемых центральным процессором (хост-программ), с периферийными устройствами возможно лишь тремя основными способами [4]:

- программно-управляемый обмен;
- прямой доступ к памяти (DMA);
- прерывания.

Во всех случаях при инициализации работы необходимы прерывания центрального процессора, инициируемые устройством или пользователем, что и можно отслеживать с помощью СЗИ.

Перечень решений

Список существующих решений и их свойств по ограничению доступа к периферийным устройствам приведен в таблице [11—19, 22—24].

Список существующих решений и их свойств

Система	Работа до/после загрузки операционной системы	Поддерживаемые платформы	Контролируемые периферийные устройства	Критерии ограничения доступа
Infowatch Traffic monitor	После	Linux, Windows	USB, DVD/CD-ROM, COM, LPT, USB, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, медиа, камеры, сканер, HID-устройства, Floppy, Smart-карта, КПК, ленточный накопитель, диски, переносные устройства Windows, Wi-Fi	Имя устройства, производитель, серийный номер
КИБ Серчинформ (SearchInform)	После	Linux, Windows	USB, DVD/CD-ROM, COM, LPT, IrDA, FireWire, модемы, Bluetooth, принтеры, медиа, камеры, сканер, HID-устройства, Floppy, Smart-карта, КПК, ленточный накопитель, подключаемые по RDP диски, переносные устройства Windows, Wi-Fi	Имя устройства, производитель, серийный номер
Zecurion Zlock	После	Windows, macOS	USB, DVD/CD-ROM, COM, LPT, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, медиа, камеры, сканер, HID-устройства, Floppy, Smart-карта, КПК, ленточный накопитель, подключаемые по RDP диски, переносные устройства Windows, Wi-Fi	Имя устройства, производитель, серийный номер, класс устройства, ID и другие (всего 15 критериев)
Symantec DLP	После	Windows	HDD, USB, COM, LPT, Wi-Fi, Bluetooth, принтеры	По регулярному выражению Device ID
GTB DLP Suite	После	Windows	USB, DVD/CD-ROM, COM, LPT, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, медиа, камеры, сканер, HID-устройства, Floppy, Smart-карта, КПК, Wi-Fi	Имя устройства, производитель, серийный номер
Falcongaze SecureTower	После	Windows	USB-устройства, съемные жесткие диски, карты памяти, локальные и сетевые принтеры, диски, подключаемые по RDP, переносные устройства Windows, Wi-Fi	ID продукта, производитель, серийный номер, модель, экземпляр, название продукта
Гарда Предприятие	После	Linux, Windows	USB, DVD/CD-ROM, COM, LPT, IrDA, FireWire, модемы, Bluetooth, принтеры, сетевые принтеры, медиа, камеры, сканер, HID-устройства, Floppy, Smart-карта, КПК, ленточный накопитель, подключаемые по RDP диски, переносные устройства Windows, Wi-Fi	Имя устройства, производитель, серийный номер, GUID
DeviceLock DLP	После	Linux, Windows, macOS	N/A	N/A
Dallas Lock	До	Windows, Linux	N/A	N/A
Secret Net (Secret Net LSP) + АПМДЗ "Соболь"	До	Linux, Windows	USB, PCMCIA, Android-устройства, IOS-устройства, биометрические устройства, контроллер магнитных дисков, ленточные накопители, IEEE 1394, внешние диски, сетевые интерфейсы, принтеры	N/A
Аккорд (Аккорд-Win64, Аккорд-X)	До	Linux, Windows	USB, PCMCIA, контроллер магнитных дисков, ленточные накопители, IEEE 1394, внешние диски, принтеры	N/A
Блокхост-МДЗ	До	Windows	USB, принтеры	N/A
Diamond ACS	До	Linux, Windows	USB, PCMCIA, Android-устройства, IOS-устройства, биометрические устройства, контроллер магнитных дисков, ленточные накопители, IEEE 1394, внешние диски, сетевые интерфейсы, принтеры	N/A

Заключение

Рассмотрены существующие решения, основными задачами которых являются контроль и мониторинг периферийных устройств. Составлен перечень шин и портов периферии, необходимых для контроля со стороны СЗИ. Рассмотрены подходы в этих системах для сохранности информации. В целом программно-аппаратные комплексы

предоставляют более высокий уровень защищенности информационной системы, чем DLP-системы, но цена на соответствующие продукты выше. Поэтому выбор решения для конкретной корпорации на данный момент неочевиден и нужно рассматривать множество факторов, так как даже с ЭВМ в связке с ПАК СЗИ хищение информации может быть легко совершено, если не проводить политику недопущения изъятия контроллера из ЭВМ.

Литература

1. Контроль доступа к USB-портам [Электронный ресурс]. URL: https://kompkimi.ru/programms-2/sistemnye-programmy/zashhita-pk/kontrol-dostupa-k-usb-portam (дата обращения: 13.10.2019).
2. *Грунтович М. М.* Работа с USB-флешками в организации. Основные ошибки [Электронный ресурс]. URL: http://www.okbsapr.ru/gruntovich_2010_7.html (дата обращения: 13.10.2019).
3. *Сычев А. Н.* ЭВМ и периферийные устройства. — Томск : ТУСУР. 2017. — 131 с.
4. *Гук М.* Энциклопедия. Шины PCI, USB и FireWire. — СПб.: ЗАО "Изд. дом "Питер", 2015. С. 16—31.
5. Интерфейсы подключения жестких дисков — IDE, SATA и другие [Электронный ресурс]. URL: http://pc-information-guide.ru/zhestkij-disk/interfejsy-podklyucheniya-zhestkix-diskov-ide-sata-i-drugie.html (дата обращения: 17.11.2019).
6. Параллельный и последовательный интерфейсы [Электронный ресурс]. URL: https://pokompam.by/razjemi (дата обращения: 17.11.2019).
7. Computer buses and interfaces [Электронный ресурс]. URL: https://www.uio.no/studier/emner/matnat/fys/FYS3240/v11/undervisningsmateriale/forelesninger/Lecture5%20%20Computer%20buses%20and%20interfaces.pdf (дата обращения: 12.12.2019).
8. Программно-аппаратный комплекс защиты информации от НСД для ПЭВМ (PC) "Аккорд-АМДЗ": Руководство администратора. 2014. — 48 с. [Электронный ресурс]. URL: https://www.okbsapr.ru (дата обращения: 20.11.2019).
9. Контроль USB-устройств [Электронный ресурс]. URL: https://www.zecurion.ru/products/zlock/application/usb-devices-control/ (дата обращения: 20.10.2019).
10. *Зайцев А. П., Голубятников И. В., Мещеряков Р. В., Шелупанов А. А.* Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие. — М.: Машиностроение-1, 2006. С. 146—178.
11. DeviceLock DLP [Электронный ресурс]. URL: https://zlonov.ru/catalog/devicelock-dlp/ (дата обращения: 12.10.2019).
12. InfoWatch EndPoint Security [Электронный ресурс]. URL: https://zlonov.ru/catalog/infowatch-endpoint-security/ (дата обращения: 12.10.2019).
13. InfoWatch Traffic Monitor [Электронный ресурс]. URL: https://zlonov.ru/catalog/infowatch-traffic-monitor/ (дата обращения: 12.10.2019).
14. Solar Dozor [Электронный ресурс]. URL: https://zlonov.ru/catalog/solar-dozor/ (дата обращения: 12.10.2019).
15. StaffCop [Электронный ресурс]. URL: https://zlonov.ru/catalog/staffcop/ (дата обращения: 12.10.2019).
16. Zecurion DLP [Электронный ресурс]. URL: https://zlonov.ru/catalog/zecurion-dlp/ (дата обращения: 12.10.2019).
17. Zlock [Электронный ресурс]. URL: https://zlonov.ru/catalog/zlock/ (дата обращения: 12.10.2019).
18. Программный комплекс ЛОГОС [Электронный ресурс]. URL: https://zlonov.ru/catalog/программный-комплекс-логос/ (дата обращения: 12.10.2019).
19. КИБ Серчинформ [Электронный ресурс]. URL: https://zlonov.ru/catalog/киб-серчинформ/ (дата обращения: 12.10.2019).
20. *Безмалый В. Ф.* Контроль над использованием внешних USB-накопителей в Windows Server 2008 [Электронный ресурс]. URL: https://www.securitylab.ru/contest/311538.php (дата обращения: 12.10.2019).
21. What Is DLP And Why Data Loss Prevention Is Important? [Электронный ресурс]. URL: https://www.devicelock.com/dlp/data-loss-prevention/data-leakage-prevention.html (дата обращения: 19.10.2019).
22. *Степанов И.* Сравнительный обзор средств предотвращения утечек данных (DLP) [Электронный ресурс]. URL: https://safe-surf.ru/specialists/article/5233/609990/ (дата обращения: 24.11.2019).
23. *Шабанов И.* Сравнение систем защиты от утечек (DLP) 2014. Ч. 1 [Электронный ресурс]. URL: https://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1 (дата обращения: 24.11.2019).
24. *Панасенко А.* Сравнение сертифицированных средств защиты информации от несанкционированного доступа для серверов и рабочих станций (СЗИ от НСД) [Электронный ресурс]. URL: https://www.anti-malware.ru/compare/information-protection-unauthorized-access-fstek-certified (дата обращения: 24.11.2019).

Tools and means for monitoring peripheral status

M. V. Pakhomov
Moscow Institute of Physics and Technology (National Research University),
Dolgoprudny, Moscow region, Russia

Studied tools and tools for monitoring the status of peripheral devices of employees of large companies. The classification of types of peripheral devices in accordance with their purpose is established. The existing solutions for controlling computer interfaces are described: options and software systems built into the operating system (OS) that work in the OS before loading it. The approaches implemented in these tools are shown. The list of the most famous products for peripheral control is received. This list contains information about the list of peripheral devices and computer interfaces that can be controlled by a specific information security tool (SIS).

Keywords: peripherals, USB, SZI, DLP, interface control, monitoring of peripheral devices.

Bibliography — 24 references. *Received April 15, 2020*

УДК 002.5

Защищенное удаленное управление

А. А. Оголюк, канд. техн. наук; *Н. М. Малкина*
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия

Рассмотрены решения для удаленного доступа к компьютеру. Проведено сравнение различных программных и аппаратных средств. Предложено создание нового продукта. Приведен набор характеристик, необходимый для реализации этого решения.

Ключевые слова: удаленный доступ, Intel, Orange Pi, Intel ME, UEFI, уязвимости.

Удаленное управление играет важную роль в администрировании компьютеров. Парк компьютеров серьезной организации может достигать нескольких сотен машин, которые порой расположены за тысячи километров друг от друга. Поддержание работоспособности системы является жизненно важной задачей для каждого отдела автоматизации.

Программное обеспечение удаленного рабочего места, более точно называемое программным обеспечением удаленного доступа или программным обеспечением удаленного управления, позволяет удаленно управлять одним компьютером с другого. Легкое подключение к удаленному компьютеру, удобство использования и возможность передачи файлов — вот основные характеристики программ удаленного управления компьютером (Remote Control Software).

Цель работы — анализ и сравнение существующих решений для удаленного доступа к компьютеру, поиска плюсов и минусов, предложение своего продукта, удовлетворяющего всем требованиям и не имеющего недостатков.

Проведем краткий анализ существующих программных и аппаратных решений для удаленного доступа на ПК.

Наиболее используемые программные решения

TeamViewer — одно из самых популярных приложений удаленного доступа. Нужно просто ввести ID и пароль и запустить удаленный доступ к удаленному ПК. Ключевой особенностью этого приложения является возможность обхода межсетевых экранов и NAT (трансляция сетевых адресов), поэтому можно получить доступ к ПК, у которого нет собственного "белого" IP-адреса (или скрыт за брандмауэром). Однако, TeamViewer имеет ряд серьезных недостатков, например закрытый исходный код. ПО с закрытым исходным кодом является проприетарным ПО. Поэтому нет гарантии, что недокументированные функции отсутствуют в приложении (включая ведение журнала и запись экрана). TeamViewer использует собственные серверы, которыми нельзя управлять (серверы могут регистрировать все действия и нет способа проверить это). Другим большим недостатком является высокая цена (TeamViewer бесплатен несколько часов использования, но затем он начинает отключать удаленное соединение с просьбой купить его) [1].

RealVNC — одно из старейших и широко используемых приложений для удаленного доступа, имеет много преимуществ. Это проект с открытым исходным кодом. Имеет много пользовательских версий. Может быть запущен практически на любой платформе (x86, ARM, MIPS и т. д.) и любой операционной системе (Windows, Linux, MacOS и т. д.). Ключевым недостатком его является отсутствие возможности подключения к ПК за брандмауэром или обхода NAT, что делает приложение бесполезным для большинства домашних или корпоративных сценариев [2].

Remote Desktop Protocol (*RDP*) — встроенное приложение Windows. Может подключить локальные устройства к удаленному ПК. Исходный код недоступен. RDP не может проходить через NAT или подключаться к ПК за брандмауэром (так же, как встроенный удаленный помощник Windows).

Аппаратные решения менее популярны из-за более высокой цены, однако это решение обеспечивает еще один уровень доступности ПК — получение удаленного доступа к ПК, когда основное питание отключено (пробуждение по локальной сети) и когда операционная система отсутствует

Оголюк Александр Александрович, доцент.
E-mail: xms2007@yandex.ru
Малкина Надежда Михайловна, студентка.
E-mail: nadine.malkina@mail.ru

Статья поступила в редакцию 18 апреля 2020 г.

или повреждена. Также есть возможность получить доступ к настройкам BIOS и параметрам загрузки, что совершенно невозможно для программных решений.

Основное аппаратное решение для ПК — встроенное решение Intel. Оно состоит из программной части, встроенной в Intel Management Engine (ME), и аппаратных компонентов, встроенных в каждую материнскую плату ПК (с чипсетами Intel, датированными 2006—2020 гг.) [3]. Аппаратная часть состоит из следующих компонентов:

- хост-микроконтроллер (включает встроенное ПЗУ);
- прошивка SPI cheap, которую частично используют совместно с основным унифицированным расширяемым интерфейсом прошивки BIOS firmware;
- выделенная оперативная память (около 32 Мб);
- унифицированный расширяемый интерфейс прошивки BIOS DXE, SME-модули;
- интерфейс модуля управления (интерфейс основного размещенного кода процессора для контроллера);
- специальный сетевой контроллер для прямого доступа к адаптеру Ethernet.

Исходный код для программной части (часть ME UEFI BIOS) недоступен. Некоторые части кода Intel ME защищены аппаратно, поэтому нет возможности извлечь их для анализа. Аппаратные компоненты скрыты в чипсете материнской платы, а их прошивка недоступна.

Самым непонятным является то, что код удаленного доступа (часть прошивки ME) присутствует в любом BIOS UEFI (на любом ПК 2009—2020 гг.), но на потребительских ПК он отключен. Удаленный доступ активен только на материнских платах серверного класса и самых дорогих ПК. Из соображений безопасности такое присутствие неактивного кода представляет серьезную угрозу.

Второй важный недостаток — уязвимости UEFI BIOS (особенно в коде удаленного доступа BIOS). Один из таких недостатков был обнаружен в 2017 году.

Все компьютеры на базе Intel Unified Extensible Firmware Interface уязвимы для него. Он находится в подсистеме Active Management Technology (модуль веб-панели).

Подсистема Active Management Technology реализует веб-сервер (для целей удаленного доступа). Веб-доступ защищен паролем. Однако было обнаружено, что код, который проверяет пароль для веб-сервера, просто разрешает вводить пустой ответ авторизации и утверждает, что он действителен.

Эта уязвимость присутствует на всех компьютерах с UEFI на базе Intel, что позволяет осуществлять несанкционированный удаленный доступ. Даже если веб-сервер выключен (подсистема удаленного доступа находится в отключенном состоянии), возможна аналогичная локальная эскалация. Это приводит к тому, что каждый современный (с 2010 по 2017 гг.) компьютер на базе Intel уязвим. Некоторые производители выпустили обновления прошивки (которые необходимо реализовать, чтобы устранить уязвимость). Многие поставщики этого еще не сделали. Та же проблема (отсутствие обновлений) актуальна для старых моделей (более 3 лет), которые уже не поддерживаются. Единственное доступное решение — прекратить их использование.

Существует несколько других аппаратных решений, таких, как Altusen IP900x PCI- платы. Аппаратные параметры: 32-разрядный процессор (266 МГц, 400 MIPS MMU, кэш-память 32 КБ), ОЗУ 32 МБ, память 16 МБ, Ethernet/LAN 100 Мбит/с, USB-концентратор, RTC, RS-485, форм-фактор PCI, 15 Вт [4]. Их ключевые особенности перечислены в таблице.

Сравнительная таблица существующих решений

Решение / Особенность	VNC	RDP	TeamViewer	Intel	Altusen IP9001	Proposed solution
Способность работать без ОС/способность войти в BIOS	–	–	–	+	+	+
Кроссплатформенность	+	–	+	+*	+–	+
Открытый исходный код	+	–	–	–	–	+
Известные уязвимости	–	+	–	++	–	Еще не реализовано*
Шифрование трафика	–	+	+	+	–	+
Поддержка USB-устройств	–	+	–	–	–	–
Поддержка файловых операций	+	+	+	–	–	+
Способность пройти через NAT/firewall	–	–	+	–	–	+
Отсутствие недокументированных функций	+	–	–	–	–	+
Бесплатно или низкая цена	+	+	–	–	–	+

* Intel работает только на платформе x86

Проанализировав показатели различных продуктов из таблицы, можно сделать вывод о том, что хорошего инструмента удаленного администрирования, объединяющего все эти критерии, не существует. Авторы предлагают решение, которое будет удовлетворять всем параметрам таблицы.

Требования к продукту

Программное обеспечение с открытым исходным кодом. Исходный код таких программ доступен для просмотра, изучения и изменения, что позволяет убедиться в отсутствии уязвимостей и неприемлемых для пользователя функций (например, скрытое отслеживание пользователя программы). Можно участвовать в доработке открытой программы, использовать код для создания новых программ и исправления в них ошибок.

Кроссплатформенность, т. е. способность программного обеспечения работать с двумя или более аппаратными платформами и (или) операционными системами. Следует иметь в виду, что существует огромное количество различных операционных систем, поэтому предлагаемый продукт должен соответствовать требованиям любой ОС.

Способность работать без ОС/способность войти в BIOS. В случае, если пользователю необходимо войти в BIOS или перезагрузить удаленный компьютер, предлагаемое решение сможет предоставить эту возможность.

Шифрование трафика. Для защиты передаваемой информации инструмент дистанционного управления должен обеспечивать шифрование трафика. Если трафик зашифрован, его могут прочитать только отправитель и получатель (собеседник на другом конце провода или сервер, на котором расположена необходимая информация) и никто другой, будь то государство или злоумышленники.

Способность проходить через NAT/firewall. Частные "серые" IP-адреса предназначены для использования в локальных сетях. Прямой доступ к Интернету с использованием частного IP-адреса невозможен. В этом случае подключение к Интернету осуществляют через NAT (трансляция сетевых адресов заменяет частный IP-адрес на общедоступный). Поэтому решение должно позволять работать за NAT/firewall.

Бесплатно или низкая цена. Для предлагаемого продукта будет использован недорогой мини-компьютер Orange Pi, из-за чего цена решения окажется невысокой.

Предлагаемая архитектура включает:

- одноплатный мини-компьютер (Orange Pi/Raspberry Pi);
- эмуляцию устройства usb-hid клавиатуры (arduino);
- устройство захвата видео (HDMI/DVI/порт дисплея/VGA);
- клиент-серверную архитектуру.

Схематичное изображение предлагаемого решения в виде блок-схемы приведено на рисунке.

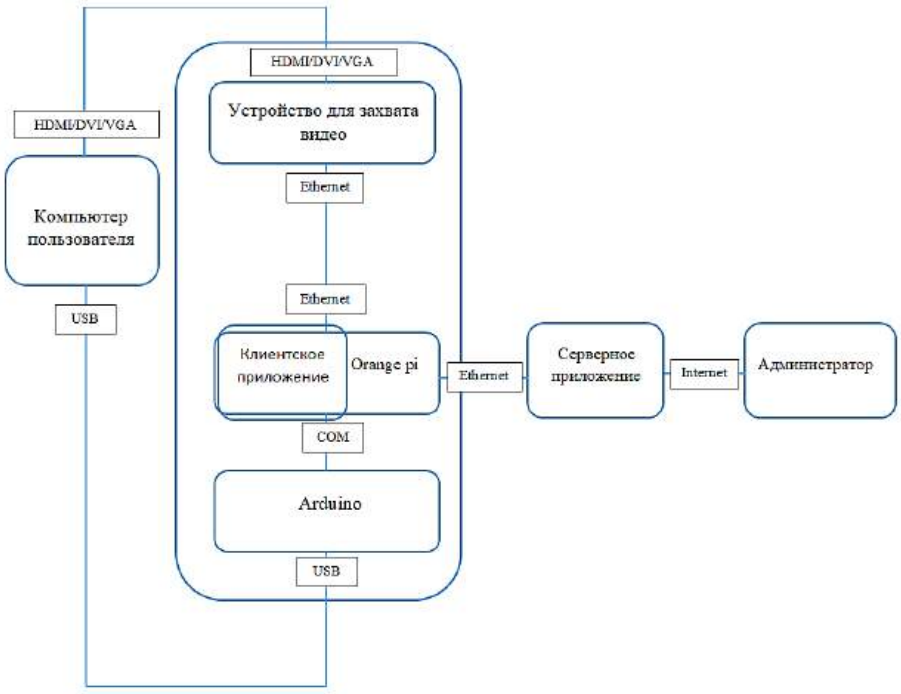


Схема разрабатываемого устройства

Литература

1. https://www.teamviewer.com/ru/
2. https://discover.realvnc.com/remote-access-tutorial
3. https://www.intel.ru/content/www/ru/ru/homepage.html
4. https://www.hwp.ru/articles/Altusen_IP9001__polniy_udalenniy_kontrol_za_serverom_ili_rabochim_kompyuterom/

Secure remote control

A. A. Ogolyuk, N. M. Malkina
St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia

This article discusses modern solutions for remote computer access. A comparison of different software and hardware is given, then the creation of a new product is proposed. The end is a set of characteristics needed to implement this solution.

Keywords: remote access, Intel, Orange Pi, Intel ME, UEFI, vulnerabilities.

Bibliography — 4 references. *Received April 18, 2020*

УДК 004.932.72'1

Анализ термограмм лица и шеи для распознавания состояния сонливости пользователей на основе классификатора Байеса

С. С. Жумажанова; *А. Е. Сулавко*, канд. техн. наук; *Д. В. Лукин*
ФГБОУ ВО "Омский государственный технический университет", г. Омск, Россия

Приведены результаты исследований по идентификации с помощью методов термографии в совокупности с методами распознавания образов и искусственного интеллекта состояния сонливости пользователей. Проведен анализ разработанного пространства признаков и алгоритмов принятия решений на базе последовательного применения формулы гипотез Байеса.

Ключевые слова: ИК-термография, термоизображения, психофизиологическое состояние, сонливость, пространство признаков, формула гипотез Байеса.

Рост уровня компьютеризации общества ведет к возникновению различного рода информационных угроз в информационных системах и сетях, а также автоматизированных системах управления. Это затрагивает сферы здравоохранения, науки, финансов (банки), топливно-энергетического комплекса, атомной энергии и т. д. (так называемые объекты критической информационной инфраструктуры — КИИ) [1]. При моделировании угроз на объектах КИИ помимо угроз неантропогенного (технического) характера необходимо рассматривать "человеческий фактор". Оператор, являясь основным звеном информационной системы, может допускать ошибки из-за нестабильного физического и/или эмоционального состояния, что создает дополнительные уязвимости для реализации угроз информационной безопасности, в крайнем случае — техногенных катастроф. По данным ИМАШ РАН [2], человеческий фактор имеет высокий показатель значимости (в долях) с точки зрения его причинно-следственной связи с авариями следующей специфики: военная авиация — 0,85; автомобильный транспорт — 0,80; гражданское и промышленное строительство — 0,70; гражданская авиация — 0,65; ядерная энергетика — 0,55; технологическое оборудование — 0,40; военная космическая техника — 0,35; трубопроводный транспорт — 0,30. Согласно данным международной статистики основными причинами техногенных аварий являются усталость [3], сонливость [4], алкогольное опьянение [5], стресс [6] (рис. 1).

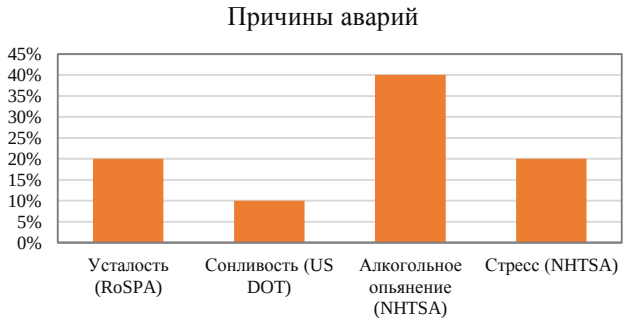


Рис. 1. Доля участия человеческого фактора в различных авариях по данным международных организаций

Состояние сонливости во время управления системами в составе объектов КИИ снижает уровень бдительности оператора, создавая опасные ситуации, и увеличивает вероятность возникновения аварий. Разработаны различные методы мониторинга состояния человека: методы лазерного мониторинга, электромагнитные и сверхширокополосные системы, системы мониторинга на основе изображений и т. д.

Методы тепловой инфракрасной визуализации используют в качестве инструмента для бесконтактной и неинвазивной вычислительной оценки вегетативной нервной деятельности человека и его психофизиологического состояния (ПФС). Анализ теплового изображения человека (в особенности лица субъекта) все чаще используют при реализации контрольно-пропускной функции. Параметры термограмм лица рассматривают как перспективные биометрические характеристики, которые содержат информацию как о личности, так и о состоянии человека.

Благодаря новому поколению высокочувствительных инфракрасных тепловых детекторов и

Жумажанова Самал Сагидулловна, аспирантка.
E-mail: samal_shumashanova@mail.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Лукин Денис Вадимович, студент.
E-mail: azlukinza@gmail.com

Статья поступила в редакцию 18 марта 2020 г.

разработке вычислительных моделей автономного контроля температуры кожи лица и других частей тела с помощью теплового инфракрасного изображения можно рассчитать различные параметры, включая локализованную скорость перфузии крови, частоту сердечных сокращений, частоту дыхания, судомоторные и стрессовые реакции. Фактически все эти параметры влияют на контроль температуры кожи. Система регуляции цикла сон—бодрствование имеет четыре ключевых механизма: бодрствования, медленно-волнового сна (МВС), парадоксального сна (ПС) и внутрисуточной ритмики. Согласно современным данным бодрствование и МВС относят к одной группе функциональных состояний, а ПС рассматривают как отдельное функциональное состояние. При этом температура мозга и температура "ядра" снижаются во время МВС за счет падения метаболической теплопродукции, что происходит постепенно по мере перехода организма из активного бодрствования в МВС, т. е. является результатом смены функционального состояния [7].

Лекарства, вводимые с седацией, стимулируют вазодилатацию терморегуляторных артериовенозных шунтов, что приводит к перераспределению тепла от ядра к периферии. Еще один механизм, с помощью которого прием седативных, анальгетических и анестезирующих средств может снизить температуру тела, — это снижение скорости метаболизма [8]. Они способствуют потере тепла за счет вазодилатации. Эти лекарства и их производные в зависимости от дозы напрямую влияют на терморегуляцию гипоталамуса [9].

Цель исследования — оценка параметров термограмм субъектов для распознавания состояния сонливости на основе алгоритма последовательного применения формулы гипотез Байеса.

Результаты оценки состояния сонливости на основе параметров термограмм

В работе [10] исследовали частоту дыхания водителей транспортных средств с использованием тепловидения. Полученное видео, снятое в тепловом диапазоне, было преобразовано в последовательность изображений. Обнаружение лица и отделение от фона выполняли с использованием алгоритма Bakhoda [11] на основании порогового метода. Область под носом была выбрана как центральная область лица. Поскольку поиск выполняли только в центральной области, считалось, что область с самой высокой температурой соответствует периорбитальной области, а область с самой низкой температурой — это нос. Два пикселя, которые представляют центр двух областей с высокой температурой и не расположены близко друг к другу, были выбраны в качестве углов глаза. Сегмент линии был нарисован путем соединения этих двух пикселей. Пиксель, расположенный на перпендикулярном бисекторе этого отрезка и имевший самую низкую температуру, был выбран в качестве кончика носа. Область непосредственно ниже кончика носа служила целевой зоной дыхания. Сигнал дыхания был построен путем связывания средней температуры области ноздрей для всех кадров. Среднее значение и среднеквадратичное отклонение частоты дыхания извлекали из сигнала дыхания с двухминутными интервалами. Частота дыхания, оцененная с помощью тепловидения, была сильно коррелирована с контрольным методом. Все точки разброса находились в пределах 95 % линий согласования. Результаты показали, что частота дыхания субъектов снизилась на 1,5 уд./мин в сравнении с состоянием бодрствования. По утверждению авторов, пространственно-временные алгоритмы более устойчивы по сравнению с пространственными алгоритмами.

В работе [12] приведены исследования по идентификации состояния сна с помощью системы из двух камер: инфракрасного сканера и инфракрасной камеры с линзой IR-Cut и решеткой инфракрасного освещения. Систему использовали для измерения частоты дыхания (ЧД) и сердечных сокращений (ЧСС). Отмечено, что спектры мощности Фурье этих двух физиологических показателей не перекрываются, что позволяет одновременно анализировать ЧД и ЧСС. Путем анализа линейной регрессии удалось достичь значения коэффициентов детерминации 0,831 и 0,95 относительно состояния покоя для ЧД и ЧСС соответственно. Представленные результаты — многообещающие, однако не исследована методика интерпретации сонного состояния по полученным показателям ЧД и ЧСС, поскольку велика вероятность аналогичных данных для других состояний, которые не подлежали рассмотрению. К тому же анализу подвергали только области рта и носа.

Физиологическую информацию, полученную с помощью этого подхода, можно использовать для определения иных психофизиологических или эмоциональных состояний, что подтверждает растущее число исследований в области психофизиологии и нейронаук, в которых используют тепловую инфракрасную визуализацию (см. таблицу).

Достигнутые результаты по идентификации ПФС за последние 5 лет

Автор/год	Распознаваемое ПФС	Регионы (ROI)	Признаки	Классификатор/ результат
Latif (2016) [13]	Аффективные состояния	Супраорбитальная и периорбитальная области, нос, рот	Признаки получены с помощью матриц уровня серого (GLCM), итого 460800 признаков для каждого ROI	60—99 %, наилучший результат получен с помощью k-NN
Koukiou (2017) [14]	Алкогольное опьянение	20 точек на лице	Значения пикселей в 20 точках	ИНС, 87 %
Hermosilla (2018) [15]	Алкогольное опьянение	22 точки пересечения вен и капилляров на лице	Средняя интенсивность 3 × 3 пикселей вокруг каждой точки сетки	Байесовский классификатор на основе моделей гауссовой смеси, 87 %
Goulart (2019) [16]	Отвращение, страх, счастье, грусть, удивление	Лоб, кончик носа, щеки, подбородок, периорбитальная и периназальная области	Среднее значение температуры, дисперсия и средние значения коэффициента излучения	LDA, средняя точность 85 %
Cho (2017) [17]	Психологический стресс, вызванный тестом Струпа	Область носа	Признаки получены из спектрограмм вариабельности глубокой сверточной нейронной сетью (CNN)	CNN, 84,59 % при различении двух уровней стресса и 56,52 % при различении трех уровней
Cruz-Albarran (2017) [18]	Гнев, отвращение, страх, радость, грусть	Область лица	Биомаркеры для каждой ROI, которые сигнализируют о появлении эмоции	Иерархический классификатор, 89,9 %
Lopez (2017) [19]	Усталость, вызванная физической нагрузкой	Область лица	Признаки, полученные с помощью CNN	SVM, 80 %

Анализ указанных и многих других работ показал, что имеются ограничения существующих методов обнаружения ПФС по термографическим изображениям: для извлечения идентификационных признаков используют отдельные области лица; относительные изменения температуры (корреляции) между областями не анализируют; расчет признаков информативности не проводят; анатомические особенности кровенаполнения областей лица и шеи учитывают редко.

Решением вопроса повышения эффективности тепловизионных систем в задачах распознавания ПФС являются:

- разработка программы и методики проведения натурных экспериментов для ввода испытуемых;
- формирование информативного пространства признаков ПФС из выделенных участков лица;
- оценка алгоритмов принятия решений, основанных на последовательном применении формул гипотез Байеса и широких нейронных сетей различных функционалов для субъект-независимого распознавания (СНЗР), при котором для обучения классификатора используют примеры одних субъектов, а для распознавания — образы других пользователей.

Извлечение признаков

Для оценки эффективности использования тепловых признаков лица и шеи в задачах распознавания ПФС авторами работы составлены программа и методика проведения экспериментов. К участникам предъявляли следующие требования: отсутствие заболеваний полости рта, операций на лице и т. д. Субъекты приходили в лабораторию, где проходил эксперимент, отдыхали в течение 30 мин перед началом эксперимента, чтобы стабилизировать обмен веществ в температурных условиях лаборатории. Для ввода в состояние сонливости испытуемые принимали седативные средства (валериану, пустырник) согласно прилагаемой инструкции.

Проведена запись на тепловизор областей лица и шеи субъектов. При этом использовали ИК-камеру FLIR E60 с разрешением 320×240 пикселей, режим съемки — одновременная в инфракрасном и видимом диапазонах с термочувствительностью 50 мК и диапазоном спектра от 7,5 до 13,5 мкм, максимальная частота кадров 30 кадров/с. Программное обеспечение от производителя позволяет получать данные о температуре лица и шеи непосредственно из сделанных ИК-записей. База данных включила записи 84 человек в состояниях "норма" и "сонливость", сделанные в разные дни. Длительность съемки каждого состояния составляла несколько минут, выбранная частота кадров 7,5 кадров/с. В результате было получено в среднем 2000 изображений для каждого субъекта в каждом состоянии, 150 из которых отобраны для анализа с необходимой периодичностью.

Авторами разработан метод выявления информативных участков 26 областей лица и шеи [20]. Участки подбирают в соответствии с анатомиче-

ской информацией о расположении мышц и сосудов на лице и шее. Эти области впоследствии используют для выбора следующих групп признаков [21]:

- локальные (рассчитанные для каждой выделенной области лица в каждом кадре);
- относительные (рассчитанные как отношения признаков для двух и более областей в каждом кадре);
- статические (рассчитанные в каждом кадре локальные и относительные признаки);
- динамические (рассчитанные между соседними кадрами для одноименных выделенных областей).

Совокупность векторов указанных признаков формирует эталон субъекта в состояниях "норма" и "сонливость". В большинстве работ по идентификации субъектов или их состояний по термографическим изображениям производится анализ таких параметров пикселей, как яркость, оттенок, цвет, насыщенность и т. д. Однако данный способ не совсем корректен, поскольку цвет является только способом визуализации поверхностной температуры объекта. Соответственно идентификационный алгоритм теряет свою эффективность при замене оборудования, сбросе его настроек и т. д. С этой точки зрения целесообразно рассматривать именно такой физиологический параметр, как температура каждого пикселя на изображении в каждой выбранной области, либо более универсальную цветовую схему в градациях серого.

В ранее проведенных исследованиях по идентификации четырех состояний ("норма", "стресс", "физическая нагрузка", "алкогольное опьянение") статистическими методами на базе аналогичных признаков [21] полученные результаты были недостаточно показательными для внедрения на практике. Из-за недостатка объема обучающей выборки функции плотности распределения признаков оказались нестабильными. В данной работе в целях улучшения результатов по идентификации ПФС база данных термограмм расширена с 20 до 84 испытуемых.

Эффективность биометрической системы зависит от качества признаков. Для наиболее точной идентификации класса признаки должны более полно характеризовать конкретный класс объектов. С этой целью созданы различные методы определения информативности (качества) признаков: оценка парных площадей пересечения плотностей вероятности признаков, их взаимной коррелированности и т. д.

В работе [22] предложены шкала и способ оценки информативности признака a_j через построение функций плотности вероятности его значений и определение площадей их пересечения Sq для образов "Свой" и "Чужой". Площадь Sq переводят в собственную информацию (в битах) по формуле

$$I_{\text{bit}}(a_j) = -\log_2 \text{Sq}(a_j). \qquad (1)$$

Результаты расчета информативности признаков для всех испытуемых в исследуемых состояниях представлены на рис. 2.

Информацию о корреляционных связях можно получить путем вычисления матрицы парных коэффициентов корреляции между признаками (рис. 3). Как можно видеть, извлекаемые признаки являются почти независимыми (корреляционные связи незначительны), что позволяет применять процедуры классификации образов, основанные на "наивной" Байесовской модели.

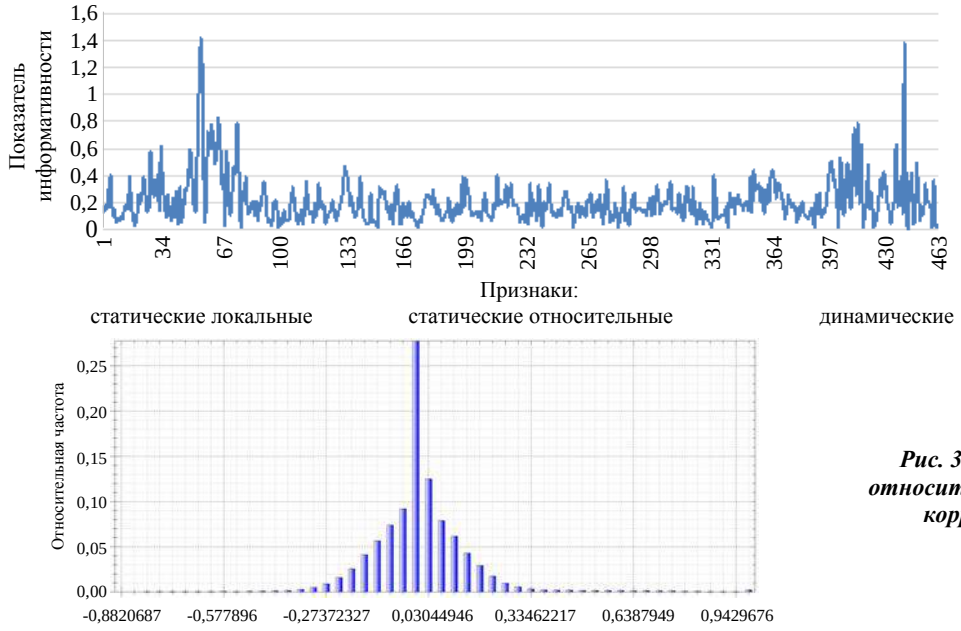


Рис. 2. Информативность 465 признаков в битах по группам

Рис. 3. Гистограмма распределения относительных частот коэффициентов корреляции между признаками

Результаты вычислительного эксперимента

Проведен вычислительный эксперимент на основании статистического подхода по оценке эффективности алгоритмов принятия решений для базы термографических изображений 84 субъектов. Определялось 2 гипотезы: "Свой" и "Чужой" (H0 и H1, соответственно). В качестве алгоритма принятия решений была выбрана формула гипотезы Байеса. Каждый эталон субъекта связан с гипотезой о его принадлежности к определенному классу (состояниям "норма", "сонливость"). Формула гипотез Байеса применяется многократно (пошагово) в зависимости от числа признаков.

$$P\left(H_i|A_j\right)=\frac{P\left(H_i|A_{j-1}\right)P\left(A_j|H_i\right)}{\sum_{i=1}^{n}P\left(H_i|A_{j-1}\right)P\left(A_j|H_i\right)} \qquad (2)$$

где $P(H_i|A_j)$ — апостериорная вероятность i-й гипотезы, рассчитанная на j-м шаге при поступлении j-го признака;

$P(A_j|H_i)$ — условная вероятность i-й гипотезы на j-м шаге (равная плотности вероятности признака [23].

На каждом шаге (j) апостериорные вероятности гипотез вычисляются с использованием формулы (2) с учетом значения одного из признаков, в то время как в качестве априорной вероятности используется апостериорная вероятность гипотезы, вычисленная на предыдущем шаге. На первом этапе все гипотезы равновероятны $P(H_i|A_0) = n^{-1}$, где n — количество гипотез. На последнем этапе предпочтение отдается гипотезе с максимальной апостериорной вероятностью.

Объем обучающей выборки составил 3 000 образов одних пользователей; для тестирования использовали 1 000 образов других пользователей. Исследования показали, что закон распределения рассматриваемых признаков близок к нормальному.

Эксперименты проводили с использованием всех признаков, а также признаков, чья информативность была выше 0,1, 0,2 и 0,3 бит. Использование признаков, информативность которых выше 0,2 бит улучшает точность распознавания системы, при добавлении признаков с информативностью ниже 0,2 бит — точность снижается. Результаты вычислительного эксперимента представлены на рис. 4.

Третий вариант оказался эффективнее, вероятность ошибок идентификации состояния сонливости составила 0,23. Использование признаков с бóльшей информативностью не дало существенного улучшения результатов. Эксперименты с аналогичным объемом обучающей и тестовой выборок, но иными наборами субъектов показали аналогичные результаты.

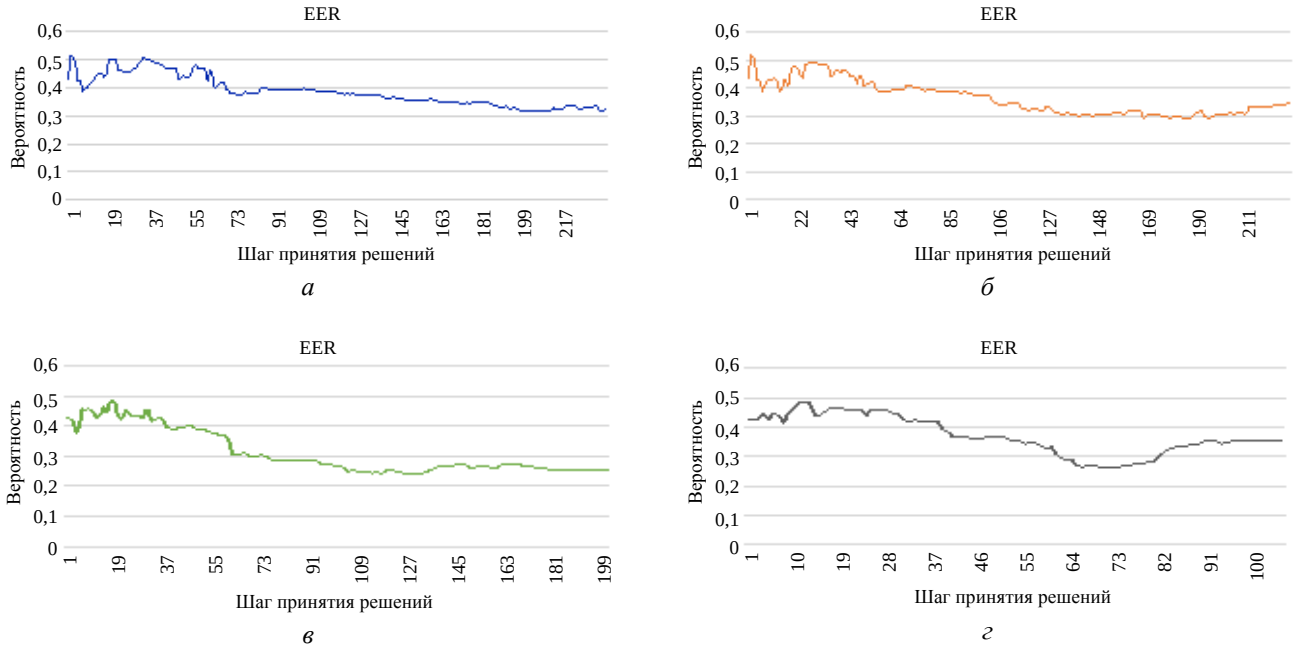


Рис. 4. Вероятность ошибок идентификации состояния сонливости:
а — с использованием всех признаков; *б* — с использованием признаков с I_{bit}>0,1 бит;
в — с использованием признаков с I_{bit}>0,2 бит; *г* — с использованием признаков с I_{bit}>0,3 бит

Заключение

Предложен метод идентификации состояния сонливости на основе модифицированной формулы гипотез Байеса. Проведены вычислительные эксперименты по оценке информативности и взаимной коррелированности признаков для оценки их "качества".

Удалось достигнуть показателей ошибок идентификации состояния сонливости 23% при использовании признаков с информативностью более 0,2 бит.

Низкая информативность признаков, извлеченных мануально, т. е. на основании знаний эксперта и эффективных на его взгляд алгоритмов и методов выделения областей интереса и признаков, позволяет в будущем рассматривать сверточные сети в качестве инструмента для автоматического извлечения признаков. Также возможен вариант комплексирования признаков, извлеченных мануально и с помощью сверточных сетей с построением классификатора нейросетевого либо Байесовского классификатора.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-37-00154.

Литература

1. Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” от 26.07.2017 N 187-ФЗ (последняя редакция) / КонсультантПлюс [Electronic resource]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed: 12.03.2020).

2. Lez’er V., Muratova I., Korpusova N. Issues of transport security and human factor. E3S Web Conf., 2019. Vol. 91. P. 08062. https://doi.org/10.1051/e3sconf/20199108062

3. Driver fatigue and road accidents — RoSPA [Electronic resource]. URL: https://www.rospa.com/road-safety/advice/drivers/fatigue/road-accidents/ (accessed: 07.10.2019).

4. Prevalence of Drowsy Driving Crashes: Estimates from a Large-Scale Naturalistic Driving Study [Electronic resource] // AAA Foundation. 2018. [Электронный ресурс]. URL: https://aaafoundation.org/prevalence-drowsy-driving-crashes-estimates-large-scale-naturalistic-driving-study/ (accessed: 08.10.2019).

5. Driving Drunk or High Puts Everyone in Danger [Электронный ресурс]: Text // NHTSA. 2017. URL: https://www.nhtsa.gov/drunk-driving/drive-sober-or-get-pulled-over (accessed: 08.10.2019).

6. The Effects of a Heavy Workload on Employees [Electronic resource] // Bizfluent. URL: https://bizfluent.com/info-8178431-effects-heavy-workload-employees.html (accessed: 08.10.2019).

7. Венцковская Е. А., Шило А. В., Бабийчук Г. А. Терморегуляция, сон и температурные воздействия // Thermoregulation, Sleep and Temperature Influences. 2010.

8. Conway A. A Review of the Effects of Sedation on Thermoregulation: Insights for the Cardiac Catheterization Laboratory // J. Perianesthesia Nurs. Off. J. Am. Soc. PeriAnesthesia Nurses. 2016. Vol. 31, № 3. P. 226–236.

9. Díaz M., Becker D. E. Thermoregulation: Physiological and Clinical Considerations during Sedation and General Anesthesia // Anesth. Prog. 2010. Vol. 57, № 1. P. 25–33.

10. Kiashari S. E. H. et al. Monitoring the Variation in Driver Respiration Rate from Wakefulness to Drowsiness: A Non-Intrusive Method for Drowsiness Detection Using Thermal Imaging // J. Sleep Sci. 2018. Vol. 3, № 1–2. P. 1–9.

11. Bakhoda H. Analysis and implementation of a new driver drowsiness detection system based on thermal infrared imaging of the face [Thesis]. Tehran, Iran: K. N. Toosi University of Technology. 2015. [In Persian].

12. Hu M. et al. Combination of near-infrared and thermal imaging techniques for the remote and simultaneous measurements of breathing and heart rates under sleep situation // PloS One. 2018. Vol. 13, № 1. P. e0190466.

13. Latif M. H. et al. Emotion detection from thermal facial imprint based on GLCM features // ARPN J. Eng. Appl. Sci. 2016. Vol. 11. P. 345–350.

14. Koukiou G. Intoxication Identification Using Thermal Imaging // Hum.-Robot Interact. — Theory Appl. 2017.

15. Hermosilla G. et al. Face Recognition and Drunk Classification Using Infrared Face Images [Electronic resource]: Research Article // Journal of Sensors. 2018. URL: https://new.hindawi.com/journals/js/2018/5813514/ (accessed: 19.12.2019).

16. Goulart C. et al. Emotion analysis in children through facial emissivity of infrared thermal imaging // PLOS ONE. 2019. Vol. 14, № 3. P. e0212928.

17. Cho Y., Bianchi-Berthouze N., Julier S.J. DeepBreath: Deep Learning of Breathing Patterns for Automatic Stress Recognition using Low-Cost Thermal Imaging in Unconstrained Settings // 2017 Seventh Int. Conf. Affect. Comput. Intell. Interact. ACII. 2017. P. 456–463.

18. Cruz-Albarran I.A. et al. Human emotions detection based on a smart-thermal system of thermographic images // Infrared Phys. Technol. 2017. Vol. 81. P. 250–261.

19. Lopez M. B., del-Blanco C. R., Garcia N. Detecting exercise-induced fatigue using thermal imaging and deep learning // 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA). 2017. P. 1–6.

20. Жумажанова С. С., Лукин Д. В., Белгородцев А. А. Разработка методики выделения участков лица и шеи на термограммах и изображениях в видимом спектре для последующего анализа в целях выявления психофизиологического состояния субъекта (Обзор) // Вопросы Защиты Информации. 2018. № 4 (123). P. 24–35.

21. Zhumazhanova S. S. et al. Statistical Approach for Subject’s State Identification by Face and Neck Thermograms with Small Training Sample // IFAC-Pap. 2019. Vol. 52, № 25. P. 46–51.

22. Sulavko A. E., Zhumazhanova S. S., Fofanov G. A. Perspective Neural Network Algorithms for Dynamic Biometric Pattern Recognition in the Space of Interdependent Features // 2018 Dynamics of Systems, Mechanisms and Machines (Dynamics). 2018. P. 1–12.

23. Епифанцев Б. Н. et al. Идентификационный Потенциал Рукописных Паролей В Процессе Их Воспроизведения // Автометрия. 2016. Vol. 52, № 3. P. 28–36.

Analysis of face and neck thermograms for users' drowsiness recognition based on the Bayesian classifier

S. S. Zhumazhanova, A. E. Sulavko, D. V. Lukin
Omsk State Technical University, Omsk, Russia

The results of identification studies using methods of thermography in conjunction with methods of pattern recognition and artificial intelligence of the state of drowsiness of users are presented. The analysis of the developed space of signs and decision-making algorithms based on the consistent application of the Bayesian hypothesis formula is carried out.

Keywords: IR thermography, thermal images, psychophysiological state, drowsiness, feature space, Bayes hypothesis formula.

Biography — 23 references *Received Match 18, 2020*

ДОВЕРЕННАЯ СРЕДА

УДК 004.93'1

Искусственный интеллект в защищенном исполнении на базе иммунных сетевых моделей распознавания образов на примере преобразователей биометрия—код

Е. В. Шалина
ФГБОУ ВО «Омский государственный университет путей сообщения», г. Омск, Россия

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

Показано, что на базе предложенных авторами моделей искусственных иммунных сетей потенциально возможно построение систем искусственного интеллекта (ИИ), устойчивых к попыткам совершения следующих действий любым неавторизованным лицом: анализ операций, совершаемых ИИ, несанкционированное управление ИИ, извлечение знаний из ИИ. Рассмотрены задачи ИИ, связанные с биометрической идентификацией и аутентификацией.

Ключевые слова: клавиатурный почерк, подпись, изображение лица, нейронные сети, комитеты классификаторов, машинное обучение, защищенные нейросетевые контейнеры.

Один из основных мировых трендов связан с развитием технологий искусственного интеллекта. Под этим термином подразумевают способность программ выполнять задачи, которые считают прерогативой человека: классификация, кластеризация, регрессия. В соответствии с Указом Президента РФ № 490 "О развитии искусственного интеллекта в Российской Федерации" поставлена задача поддержки научных исследований, направленных на решение до 2030 г. следующих задач: алгоритмическая имитация биологических систем принятия решений, в том числе распределенных коллективных систем, автономное самообучение и развитие адаптивности алгоритмов к новым задачам. К указанным направлениям относят разработку моделей:

– искусственных иммунных систем и сетей (ИИС) и алгоритмов их обучения [1];

– искусственных нейронных сетей (ИНС) и алгоритмов их обучения [2].

Шалина Екатерина Викторовна, аспирантка.
E-mail: burka-777@yandex.ru
Малинин Никита Витальевич, студент.
E-mail: niki_nv@mail.ru
Сулавко Алексей Евгеньевич, доцент кафедры "Комплексная защита информации".
E-mail: sulavich@mail.ru
Стадников Денис Геннадьевич, студент.
E-mail: sdg250598@inbox.ru

Статья поступила в редакцию 18 марта 2020 г.

Доверие к приложениям ИИ во многом определяется тем, на каких данных было проведено обучение, достаточен ли объем обучающей выборки, каким алгоритмом выполняли обучение. Важным аспектом, касающимся алгоритмов обучения, являются устойчивость и способность настроить ИИС или ИНС, даже если объем обучающей выборки ограничен. Алгоритм обучения должен быть робастным. При этом после обучения ИИС (ИНС) должна быть способна давать высоконадежные, качественные решения поставленных задач.

Комплекс указанных вопросов уже решен в России для сетей искусственных нейронов с накоплением данных в линейных пространствах и с накоплением данных в квадратичных пространствах для биометрических данных. Стандартизованы процедуры полностью автоматического обучения сетей из искусственных нейронов, осуществляющих обогащение бедных входных данных путем их накопления в линейном пространстве (ГОСТ Р 52633.5-2011). Разработан проект стандарта, регламентирующего процедуры автоматического обучения искусственных нейронов, осуществляющих обогащение бедных входных данных накоплением в квадратичном пространстве. Только после полной автоматизации процедур обучения сетей искусственных нейронов возможен переход к следующему этапу защиты таблиц обученной нейронной сети криптографическими механизмами. Положительный пример реализации криптографической защиты таблиц обученной сети искусственных нейронов с накоп-

лением в линейном пространстве отражен в соответствующей технической спецификации "Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов".

Серия стандартов ГОСТ Р 52633 относится к построению нейросетевых преобразователей биометрия—код (ПБК) [3], на базе которых должны строится средства высоконадежной биометрической аутентификации. ПБК настраивают на выдачу ключа (пароля) пользователя при предъявлении его биометрического образа. При предъявлении образа любого другого субъекта ПБК должен формировать случайный бинарный код, близкий к "белому шуму". Таким образом, ПБК имеет только одно стабильное состояние, ассоциированное с ключом (паролем) пользователя-владельца. Однако подобные решения можно использовать и для других задач интеллектуального анализа данных (пока только распознавания образов, но в перспективе и кластеризации и регрессии).

Тем не менее результаты последних исследований указывают на то, что гибридные нейронные [4] или иммунные [5] сети также способны к робастной настройке и при этом могут давать более высокоточные решения. В данной работе предложен способ защиты параметров обученных иммунных сетей путем применения обратимых и необратимых преобразований, аналогичных тем, которые применяют для защиты искусственных нейронных сетей, обученных по ГОСТ Р 52633.5 [6].

Искусственный интеллект в защищенном исполнении

Прежде всего необходимо обозначить, что такое ИИ в защищенном исполнении и для чего это нужно. Под защищенным исполнением понимают невозможность совершения следующих действий любым неавторизованным лицом или субъектом (процессом, пользователем, злоумышленником):

- анализа операций, совершаемых ИИ (алгоритм работы ИИ, суть преобразований);
- управления ИИ (с помощью изменения алгоритма работы, подмены данных ИИ и т. д.);
- извлечения знаний ИИ.

Любое несанкционированное вмешательство в работу ИИ может повлечь за собой последствия: материальный ущерб, нарушение информационной безопасности, угрозу жизни, здоровья граждан, технологические сбои или катастрофы и т. д. Все зависит от назначения конкретной реализации ИИ и возможностей, которыми данный экземпляр ИИ обладает.

Одним из перспективных направлений исследований в области защиты ИИ является гомоморфное шифрование — форма шифрования, позволяющая производить определенные математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом. Любой программный код (приложение, макрос и т. д.), зашифрованный средствами традиционной криптографии, должен быть дешифрован перед запуском на исполнение. При этом исполняемый код полностью или частично находится в расшифрованном виде в оперативной памяти компьютера (мобильного устройства). Гомоморфное шифрование позволит непосредственно выполнять зашифрованный код, как если бы он был не зашифрован.

Полноценного гомоморфного шифрования пока не разработано. Разработан аппарат частичного гомоморфного шифрования с поддержкой операций сложения и умножения. При этом исполняемый гомоморфный код оказывается в несколько тысяч раз длиннее кодов обычной программы, что не позволяет разместить его в маломощных микропроцессорах интернет-вещей, интернет-датчиков [7].

Однако если искусственный интеллект будет реализован в нейросетевом логическом базисе, то гомоморфного шифрования не потребуется. Параметры обученных ИНС (нейросетевые контейнеры) представляют собой веса входов нейронов, а также указатели на связи нейронов (синапсы) с признаками (входными параметрами ИНС) и между собой. Каждый нейрон имеет функцию активации, таблицу весовых коэффициентов и таблицу связей (таблицы нейросетевых функционалов). Восстановить обучающую выборку, а также примеры входных сигналов, которые поступали на вход ИНС, исходя из таблиц нейросетевых функционалов проблематично. То, как обученная нейронная сеть хранит свои знания о предметной области (о задаче ИИ), условно можно назвать нейросетевой криптографией. При этом никаких криптографических операций (как традиционных, так и гомоморфных) не выполняется. Кроме того, нейросетевые преобразования являются сложно интерпретируемыми сами по себе. Предсказать результат работы нейронной сети затруднительно.

Для повышения уровня защищенности нейросетевого ИИ можно применить механизм защиты нейросетевых контейнеров с использованием обратимых и необратимых преобразований. Суть этого механизма заключается в шифровании таблиц нейросетевых функционалов некоторых нейронов на ключе, который зависит от выходных значений других нейронов [6]. Защищенный нейросетевой контейнер (ЗНК) строится непосредственно по завершении процедуры обучения ИИ.

После создания ЗНК ИИ теряет способность к обучению и может работать только в режиме принятия решений. Поэтому важно, чтобы процедура настройки ИИ была робастной и гарантировано приводила к результату — появлению качественно обученного ИИ, который можно хранить в виде ЗНК и воспроизводить в защищенном режиме, либо информированию о том, что используемая обучающая выборка нерепрезентативна и ИИ не может быть обучен (требуется больше примеров).

Реализации механизмов внутренней самозащиты недостаточно. Требуется, чтобы ИИ формировал команды (управляющие сигналы воздействия на объект, который находится под контролем ИИ) так, чтобы у злоумышленника не было возможности использовать статистику по работе ИИ для получения несанкционированного контроля. Такое поведение ИИ может быть реализовано на основе концепции ПБК, но имеющего множество стабильных состояний. Каждое стабильное состояние будет представлять собой длинный криптографический ключ (пароль), который можно ассоциировать с определенным управляющим воздействием (последовательность команд может быть зашифрована на данном ключе). Любое стабильное состояние ПБК защищено, т. к. его получение сопряжено с процессом переработки входной информации в нейросетевом логическом базисе с применением механизма ЗНК.

Нечеткий экстрактор и нейросетевые ПБК

Современный человек активно пользуется средствами вычислительной техники для работы и развлечений, оставляя за собой "цифровой след". Растет число личных кабинетов и паролей, которые нужно хранить. Пользователь нуждается не только в надежной аутентификации, но и в защите аутентификационных данных от компрометации с учетом человеческого фактора. Пароли и криптографические ключи являются отчуждаемыми от владельца и поэтому подвержены действию человеческого фактора. Длинный ключ (пароль) является надежным, если только соблюдены все правила при его генерации: энтропия ключа должна быть сопоставима с его длиной. Однако случайный длинный пароль почти невозможно запомнить. Выходом из этой ситуации является привязка всех ключей и паролей субъекта к его биометрическим параметрам с помощью ПБК. Сами пароли (ключи) необходимо генерировать до обучения ПБК в соответствии с принятыми нормами. Данные обученного ПБК (ключ и биометрический эталон) должны быть защищены от компрометации при хранении и передаче по каналам связи без применения сторонних средств шифрования. Хакеры не должны иметь возможность извлечения знаний из обученного ПБК.

В стандартах по информационной безопасности описаны требования, относящиеся к защите биометрических эталонов (данных обученных ПБК) от компрометации при их хранении и передаче по каналам связи. Обобщенная схема ПБК представлена на рис. 1, *а*. Сложилось два основных подхода к построению ПБК: на основе нечеткого экстрактора (рис. 1, *б*) и широких ИНС (рис. 1, *в*). Под широкими ИНС подразумевают сети из большого количества нейронов, но малого числа скрытых слоев. Нечеткие экстракторы лежат в основе стандартов ISO/IEC 19792:2009, 24761:2009, 24745:2011, а серия стандартов ГОСТ Р 52633 базируется на широких сетях. Рассмотрим данные подходы на предмет потенциальной возможности использования для построения защищенного ИИ.

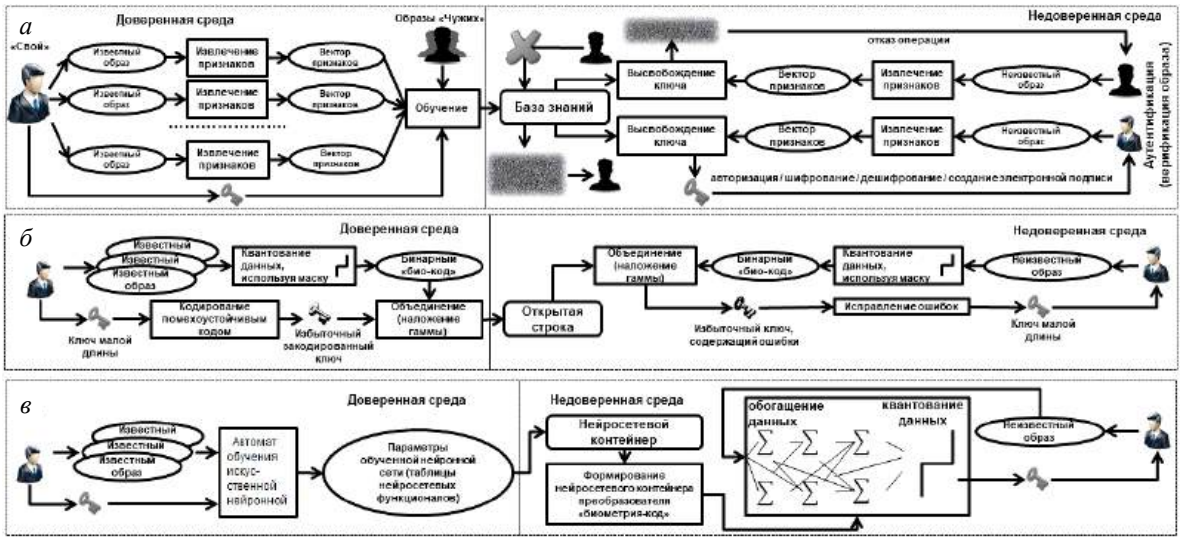


Рис. 1. Принципы работы ПБК:
а — общая схема; *б* — нечеткий экстрактор; *в* — нейросетевой ПБК

Принцип работы нечеткого экстрактора [8] основан на квантовании биометрических данных (получение биокода) и применении классических корректирующих кодов (БЧХ, Адамара и т. д.) для исправления ошибочных бит в биокоде. Такой подход не подразумевает полноценного обучения. Поэтому приемлемые результаты удается получить, только если признаки относятся к высокоинформативным (например, в задачах аутентификации по отпечатку пальца [9] или радужке [10]). При использовании в целях аутентификации менее информативных признаков (подпись [11], голос [12]) нечеткие экстракторы дают очень высокий процент ошибок. Этот подход однозначно неприменим для решения сложных задач интеллектуального анализа данных, требующих большого объема обучающей выборки и построения полноценного ИИ. Формальные недостатки данного подхода изложены в работах [3, 6, 13, 14].

Нейросетевой ПБК строят персонально для каждого субъекта. При этом формируется ИНС, количество входов которой равно числу признаков, а количество выходов — длине личного ключа субъекта (рис. 1, *в*). Каждый нейрон последнего слоя генерирует один бит. Нейронная сеть обучается на биометрических образах пользователя ("свой") и образах, не принадлежащих пользователю ("чужой"), чтобы вырабатывать ключ (пароль) субъекта при поступлении на вход его биометрического образа. Хорошо обученная нейронная сеть не нуждается в дополнительной корректировке выходов.

Обучение многослойных ИНС с помощью итерационных алгоритмов, основанных на градиентном спуске, неустойчиво, особенно при малых объемах обучающей выборки. Для настройки "глубоких" сетей требуются сотни тысяч обучающих примеров. По этой причине "широкие" сети (основа для стандартов ГОСТ Р 52633) настраивают без применения метода градиентного спуска. Идеологом и основателем этого направления является Иванов А. И. [6, 7], под авторством которого за последние 20 лет вышло множество статей и монографий. Обучение широкой сети выполняют послойно, а каждый нейрон обучают независимо от остальных нейронов. Веса входов нейрона определяют исходя из параметров распределения признаков, вычисленных по данным обучающей выборки.

Гипотетически построение нейросетевых ПБК возможно и на базе многослойных ИНС, но с использованием предобучения (рис. 2). Для этого строят автокодировщик (глубокая сверточная нейронная сеть, которая обучается на больших объемах данных).

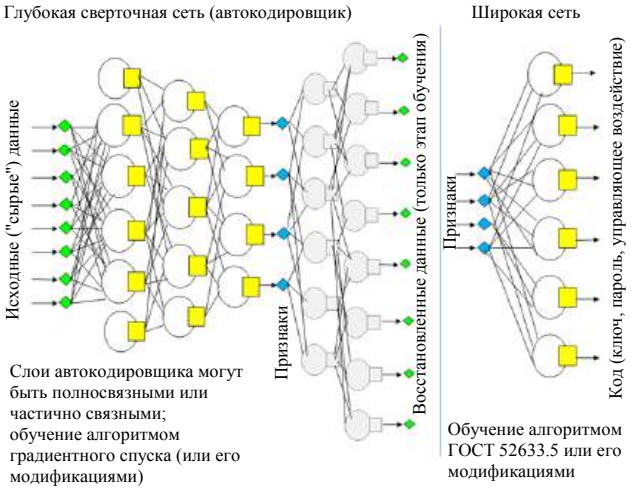


Рис. 2. Структурная схема нейросетевого ПБК, объединяющего глубокую и широкую сети. Автокодировщик обучают классическим подходом, чтобы сжимать (также можно использовать расширяющиеся или вариационные автокодировщики) и восстанавливать данные. После обучения последние слои (окрашены в серый цвет) можно удалить

Архитектура автокодировщика такова, что он способен находить закономерности в произвольных данных и извлекать информативные признаки. Далее эти признаки могут быть поданы на вход широкой ИНС, которая обучается в соответствии с принципами, изложенными в ГОСТ Р 52633.5 (алгоритм может быть усовершенствован под задачи идентификации, кластеризации и регрессии). Перспективным направлением являются разработка и исследование архитектур вариационных (нейробайесовских) автокодировщиков [15].

После обучения широкой сети из ее параметров можно сформировать ЗНК. Такой подход способен послужить основой для создания защищенного ИИ. К недостаткам данного подхода можно отнести следующие.

- При разделении нейросетевого ПБК на две составляющие (глубокую и широкую сети) их уровни защищенности будут различными. Применить механизм ЗНК можно только по отношению к широкой сети, настроенной по аналогии с алгоритмом ГОСТ Р 52633.5. Создание ЗНК на основе параметров обученной глубокой сети проблематично. Это вызовет разрыв внутренней логики многослойной ИНС, после чего сеть будет неспособна давать правильный результат. Использование ЗНК требует специальных робастных алгоритмов обучения, которые для глубоких ИНС еще предстоит разработать.
- Обученная нейронная сеть, которую формируют из ЗНК, будет работать гораздо медленнее, чем сеть, сформированная из обычного нейросетевого контейнера. Потеря производительности для

малых сетей незначительна. Для многослойных больших сетей эти потери будут ощутимы.

Иммунологический и нейросетевой ПБК

Искусственные иммунные системы (сети) в компьютерных науках принято рассматривать как семейство алгоритмов [16], основанных на соответствующих теориях о естественной иммунной системе (ЕИС): дендритных клеток, негативного отбора, клональной селекции (положительного отбора), сетевых алгоритмов (последние чаще всего называют иммунными сетями, а не системами; далее все типы иммунных моделей будем называть ИИС). Иммунная система содержит множество клеток (макрофаги, дендритные клетки, лимфоциты), которые обладают способностью обнаруживать и удалять чужеродные организмы (антигены). Назовем все такие клетки детекторами [16] — вычислительными элементами, способными анализировать распознаваемый образ либо его отдельные фрагменты и реагировать на него пропорционально тому, насколько этот образ соответствует антигену. Пусть шкала реакций детекторов задана на интервале действительных чисел [0; 1], где 0 — полная уверенность в том, что клетка принадлежит организму (гипотеза "свой"), а 1 — полная уверенность в обратном (гипотеза "чужой"). Силу взаимодействия между клетками ИИС и антигеном также называют аффинностью. Детектор является аналогом нейрона. Но в отличие от нейрона основой детектора может служить любая мера близости (функционал), в сочетании с которой можно использовать любую функцию активации, приводящую значение меры близости к интервалу [0; 1]. В основе классического нейрона всегда лежит функционал взвешенного суммирования

$$y = \sum_{j=1}^{n} \mu_j a_j, \qquad (1)$$

где a_j — значение j-го входа нейрона/детектора, связанного с определенным признаком;

μ_j — весовой коэффициент j-го входа классического нейрона, который вычисляют по формуле

$$\mu_j = \frac{\left| m_s(a_j) - m_o(a_j) \right|}{\sigma_s(a_j)\sigma_o(a_j)}, \qquad (2)$$

где $m_o(a_j)$ и $\sigma_o(a_j)$ — математическое ожидание и среднеквадратичное отклонение значений j-го признака образа "свой";

$m_s(a_j)$ и $\sigma_s(a_j)$ — аналогичные показатели образа "чужой".

Если нейрон настроен на выдачу единицы при поступлении образа "свой", то знак весового коэффициента выбирают исходя из правила: "+" при $m_s(a_j) < m_o(a_j)$, в противном случае "–". Если нейрон настроен на ноль, знаки инвертируют.

В ГОСТ Р 52633.5-2011 также предписано обязательное использование пороговой функции активации Хевисайда:

$$f(y) = \begin{cases} 0, \text{ если } y < \mu_0; \\ 1, \text{ если } y > \mu_0, \end{cases} \qquad (3)$$

где μ_0 — порог активации нейрона;

y — отклик функционала нейрона/детектора на образ "свой" или "чужой";

$f(y)$ — функция активации классического нейрона;

n — количество входов (размерность) нейрона/детектора.

Другими словами, классический нейрон представляет собой линейный классификатор (с линейной или нелинейной функцией активации), детектор же может быть как линейным, так и нелинейным классификатором.

В ИНС любой слой формируют из нейронов одного типа (с одинаковой функцией активации). Поэтому однослойный персептрон, обученный по ГОСТ Р 52633.5-2011, можно назвать комитетом линейных классификаторов. ИИС не образует конструкций в виде слоев. В данной работе рассмотрены архитектуры ИИС, объединяющие разнородные детекторы (как, например, в работе [5]), в основе которых лежат различные функционалы и/или функции активации (в этом отношении ИИС схожи с гибридными (гибкими) сетями из работы [4]). Такого рода ИИС можно назвать комитетом из разнородных классификаторов (как и гибкие сети).

Идея объединения классификаторов в комитет основана на теореме Кондорсе, которая утверждает: если мнения экспертов независимы и вероятность правильного решения каждого из них больше 0,5, то с увеличением количества экспертов вероятность правильного решения комитета экспертов возрастает и стремится к единице. При этом чем выше вероятность верного решения для каждого эксперта в отдельности, тем выше вероятность верного решения комитета. На практике решения классификаторов, играющих роль экспертов, в той или иной мере коррелированы. Чем ниже коррелированность решающих правил, тем более ощутим положительный эффект при их комплексировании. Поэтому в ИИС (как и в гибридных ИНС) целесообразно объединять разнородные (т. е. основанные на использовании различных мер близости) детекторы (нейроны).

Наиболее важным отличием ИИС от ИНС (глубоких, широких и гибридных) является алгоритм обучения. ИИС из работы [5] так же как и широкие сети обучается без применения градиентного спуска, но алгоритм настройки ИИС — итерационный. В отличие от глубоких сетей данный алгоритм достаточно устойчив. Основную идею алгоритма (и его возможных модификаций) можно описать как подбор комитета из наиболее эффективных разнородных классификаторов, которые настраивают с использованием примеров тренировочной выборки, но эффективность которых оценивают на основании валидационной (или тренировочной) выборки. Обе выборки являются непересекающимися подмножествами обучающей выборки. Таким образом, рассматриваемые архитектуры ИИС [5] можно назвать усовершенствованными гибкими сетями [4], которые настраиваются итерационно. При этом уничтожаются слабые детекторы (нейроны), а также детекторы (нейроны), которые дают сильно коррелированный результат с решениями других детекторов. Остаются сильные нейроны, решения которых менее коррелированы.

Чтобы ИИС работала в режиме ПБК, необходимо обучить комитет из N детекторов по алгоритму [5], где N — длина кода, генерируемого ПБК в битах. Далее следует заменить функцию активации каждого детектора на пороговую (3).

Результаты проведенных экспериментов показали, что гибкие гибридные сети и ПБК на их основе дают меньше ошибочных решений, чем классические нейросетевые ПБК [4]. ИИС потенциально должны давать еще меньший процент ошибок по сравнению с гибкими сетями [5]. Кроме того, ИИС должны работать быстрее (так как отбирается ограниченное количество только наиболее сильных разнородных детекторов).

При осуществлении доступа к параметрам $m_o(a_j)$ злоумышленник может фальсифицировать биометрический образ субъекта, изготовив цифровой "муляж". Поэтому параметры $m_o(a_j)$, $\sigma_o(a_j)$, $m_s(a_j)$ и $\sigma_s(a_j)$ после обучения нейросетевого ПБК удаляют, чтобы не компрометировать эталон. Остаются таблицы связей и весов μ, из которых нельзя непосредственно вычислить $m_o(a_j)$. Таким образом, обучить нейросетевой ПБК по ГОСТ Р 52633.5-2011 означает вычислить по данным обучающей выборки параметры распределения признаков $m(a_j)$, $\sigma(a_j)$ и далее по ним вычислить веса μ_j и μ_o каждого нейрона (удалив после процедуры настройки $m(a_j)$, $\sigma(a_j)$).

Функционалы, которые применяли в работе [5] для построения детекторов, непосредственно использовали параметры $m_o(a_j)$, $\sigma_o(a_j)$ для расчета близости предъявленного образа к эталону "свой" и "чужой" (например, меры Евклида, Пирсона и другие не позволяют перейти от $m_o(a_j)$, $\sigma_o(a_j)$ к весам μ). Поэтому для построения детекторов в иммунологическом ПБК предложено использовать параметрические функционалы

$$y = \sum_{j=1}^{n} \mu_j \, a_j^g; \tag{4}$$

$$y = \sum_{j=1}^{n} \left| \frac{a_t}{\sigma_s(a_t)} - \frac{a_j}{\sigma_s(a_j)} \right|^g; \tag{5}$$

$$y = \sqrt[g]{\sum_{j=1}^{n} \left| \frac{a_t}{\sigma_s(a_t)} - \frac{a_j}{\sigma_s(a_j)} \right|^g} \tag{6}$$

где g — степенной коэффициент, влияющий на характер вычислений.

Данные функционалы могут заменить разнообразные меры близости из работы [5], их предполагают сочетать с функцией активации (3). Настройка детектора на базе функционала (4) может быть аналогична настройке детектора с функционалом (1), но с учетом возведения a_j в степень g (при $g = 1$ эти функционалы становятся идентичными). Меры близости (5) и (6) можно отнести к многомерным функционалам Байса [14], так как они имеют идентичные свойства (совершают тем меньше ошибок классификации "свой"/"чужой", чем выше коэффициенты парной корреляции между признаками под номерами t и j). Предлагаемый вариант многомерных функционалов Байеса компрометирует только $\sigma_s(a_j)$ — среднеквадратичные отклонения признаков для эталона образов "чужой", которые злоумышленник может самостоятельно вычислить, используя большие выборки биометрических данных. Параметр g не компрометирует биометрический эталон и связанный с ним ключ (пароль) субъекта. Таким образом, обученные детекторы Байеса хранят необходимую информацию о классах образов в виде параметров $\sigma_s(a_j)$, g и μ_0 (порог активации детектора). Порог μ_0 следует задавать исходя из корреляции признаков и откликов на образы "свой" или "чужой" из обучающей выборки (в зависимости от того, единичный или нулевой бит должен генерировать детектор). Слабокоррелированные признаки нужно обрабатывать с помощью меры близости (4).

Защита нейросетевых и иммунных контейнеров

Нейросетевые ПБК обладают одним нежелательным свойством, которое приводит к возможности реализации атак на извлечение знаний из нейросетевого контейнера.

В ГОСТ 52633.3-2011 изложена методика тестирования нейросетевых ПБК на устойчивость к атакам на извлечение знаний. Согласно стандарту в эксперименте необходимо использовать не только естественные образы "чужой", но и синтетические, генерируемые на основе скрещивания естественных (по методике ГОСТ 52633.2-2010). При скрещивании следует выбирать пары из 1 % "чужих", наиболее близких в метрике Хемминга к образу "свой". Далее по аналогичному принципу можно скрещивать синтетические образы. Каждая новая популяция все ближе к образу "свой". В процессе тестирования по ГОСТ 52633.3-2011 сокращается количество попыток предъявления конкурирующих примеров, а точность оценки FAR (вероятности ошибки ложного допуска) возрастает на порядки при сохранении статистической значимости. Хакер может собрать базу примеров естественных образов "чужой" большого объема (речь идет о тысячах примеров), провести тестирование по ГОСТ 52633.3-2011 и, проведя вычислительный эксперимент по распознаванию примеров образов "чужих" в пакетном режиме, оценить среднюю стабильность генерируемых кодов для каждого "чужого" по формуле

$$y = \sum_{l=1}^{L} 2\,|\,P_l(1) - 0{,}5\,|, \qquad (7)$$

где L — количество нейронов/детекторов;
l — номер нейрона/детектора;
$P_l(1)$ — вероятность (или относительная частота) появления единицы (можно заменить на $P_l(0)$) в l-м разряде ключа, генерируемого примером образа k-го "чужого".

На рис. 3 продемонстрирована возможность проведения такой атаки на нейросетевой контейнер, обученный на примерах образов подписи, а на рис. 4 — аналогичной атаки на иммунный контейнер. Показатели стабильности для каждого "чужого-k" вычисляли по 10 примерам его образа.

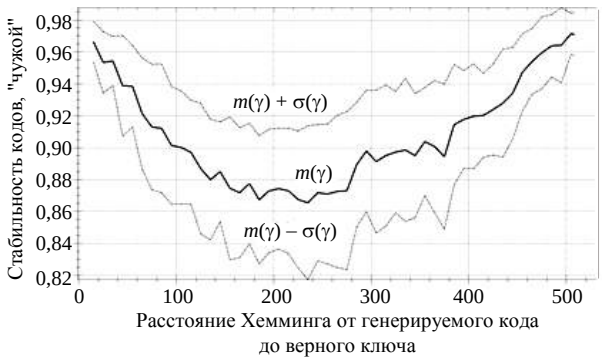


Рис. 3. Стабильность кодов "чужой-k" в зависимости от числа неверных бит в генерируемом ключе (для нейросетевого ПБК)

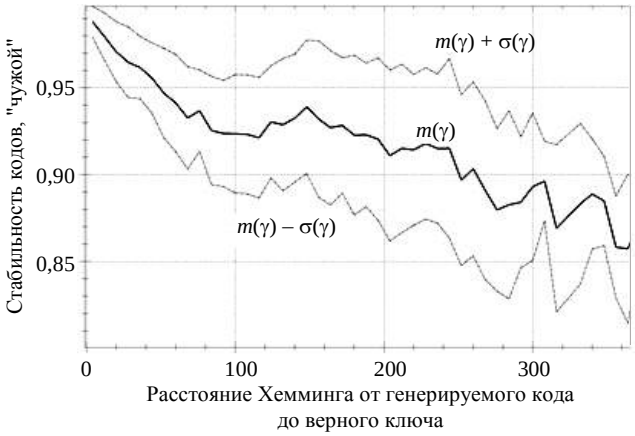


Рис. 4. Стабильность кодов "чужой-k" в зависимости от числа неверных бит в генерируемом ключе (для иммунологического ПБК)

По результатам эксперимента стабильность кодов "чужой" (7) оказывается связанной с числом неверных бит ключа. Таким образом, метрика стабильности (7) является косвенным индикатором близости генерируемых ключей к ключу пользователя. Хакер может осуществить направленный перебор синтетических образов, скрещивая примеры паролей разных "чужих", которые дают наиболее стабильный выходной код сети по методике ГОСТ 52633.2-2010. Через несколько поколений скрещивания, двигаясь в сторону повышения стабильности кода, почти всегда удается подобрать "чужого", почти идентичного образу "свой". Различие в рис. 3 и 4 состоит в том, что при взломе нейросетевого контейнера злоумышленник может осуществлять направленный перебор образов сразу по двум направлениям: к образу "свой" и к его инверсии. Инверсия образа "свой" дает обратный код на выходе нейросетевого ПБК, который можно инвертировать и получить искомый ключ (пароль). Таким образом, направленный перебор ускоряется в 2 раза. Иммунологический контейнер таким свойством не обладает, однако его взлом тоже возможен, но занимает в 2 раза больше времени. По этой причине иммунологический ПБК предпочтительней. Аналогичную атаку можно провести, используя для индикации близости меру точечной энтропии [6].

Для защиты от данной атаки Иванов А. И. и соавторы [3, 6] предлагают защищать нейросетевые контейнеры путем размножения ошибок образа "чужой" с применением обратимых и необратимых преобразований. Аналогичный принцип можно применить для защиты иммунных контейнеров (ЗИК). Детекторы можно выстроить в цепочку, как показано на рис. 5.

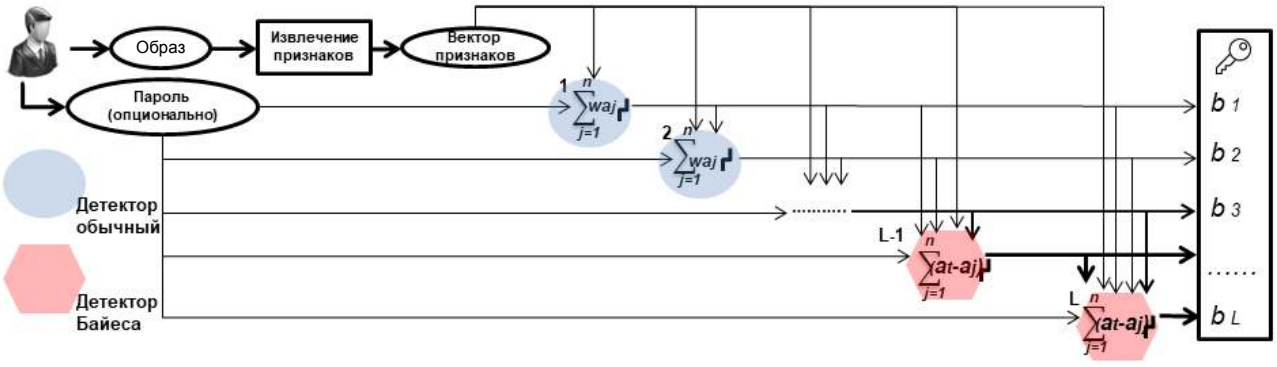


Рис. 5. Механизм ЗИК. Каждый следующий детектор связан со всеми предыдущими. Так детекторы последовательно расшифровывают связи и веса последующих нейронов и детекторов

После обучения ПБК таблицы каждого детектора шифруют наложением гаммы, представляющей собой контрольную сумму выходов всех предыдущих детекторов в цепочке:

$$\text{tables}_l' = \text{XOR}(\text{tables}_l, \text{hash}(\text{pass}, b_1, ..., b_{l-1})), \quad (8)$$

где b_l — выход, на который настраивают l-й детектор в цепочке;
hash(…) — криптографическая хеш-функция (например, md5);
tables_l — таблицы параметров l-го детектора;
pass — пароль, который является опциональным и служит для дополнительной 2-факторной защиты.

В режиме ЗНК один неверно сгенерированный бит ключа приводит к лавинообразному накоплению ошибок и хешированию данных кода "чужой", что повышает его энтропию (рис. 6).

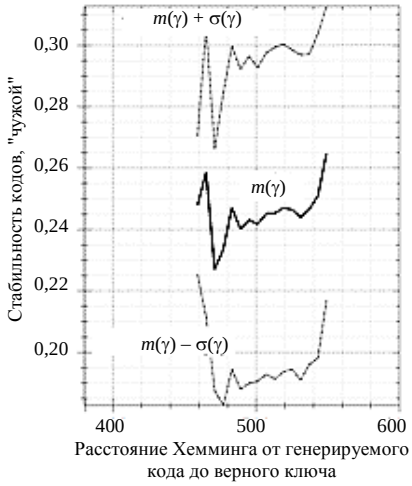


Рис. 6. Стабильность кодов "чужой-k" в зависимости от числа неверных бит в генерируемом ключе в режиме ЗИК (для иммунологического ПБК)

Стабильность кодов "чужой" становится низкой и перестает возрастать с приближением к коду "свой". Принципиальным является то, что детекторы на базе функционала (4) следует размещать в начале цепочки (см. рис. 5), а остальные (байесовские) детекторы — в конце (как менее защищенные, так как они компрометируют $\sigma_s(a_j)$ и, отчасти, информацию о высокой коррелированности признаков t и j).

Биометрическая идентификация и аутентификация на основе иммунных сетей в режиме ЗИК

В рамках исследования разработаны имитационная модель системы биометрической идентификации и аутентификации на основе ИИС (с использованием режима ЗИК и без него), а также программный комплекс, который реализует данную модель. Модель можно применять для любого пространства признаков. В рамках работы реализована возможность использования в качестве биометрических образов двухмерных изображений лица и данных клавиатурного почерка при наборе парольных фраз. Лицо является открытым биометрическим образом, поэтому его целесообразно использовать в целях идентификации. Клавиатурный почерк — это тайный образ, который можно использовать для аутентификации. Проведенные вычислительные эксперименты с использованием баз изображений лиц и клавиатурного почерка (данные 90 испытуемых, собранные авторами) показали следующие значения средней вероятности ошибок 1-го и 2-го рода:

- идентификация по лицу (без режима ЗИК) 0,0029;
- аутентификация по клавиатурному почерку (в режиме ЗИК) 0,045.

В режиме идентификации для каждого субъекта формируют отдельную ИИС (по аналогии с аутентификацией), а предъявляемый биометрический образ передают в каждую из ИИС. Результат принимают в пользу того субъекта, иммунная сеть которого дает наименьший отклик. В режиме

аутентификации сравнение осуществляют "один к одному". При этом ИИС работает как ПБК, который инициализируется из ЗИК.

Заключение

Защищенные нейросетевые контейнеры являются самым надежным средством защиты биометрических образов пользователей [3, 6]. Альтернативой являются нечеткие экстракторы, которые значительно уступают нейросетевым ПБК по надежности распознавания образов пользователей и уровню защиты биометрических эталонов. Этот тезис подтвержден многочисленными исследованиями [3, 6, 13, 14]. Однако нейросетевые ПБК несколько уступают по точности распознавания субъектов гибридным сетевым методам [4], к которым относятся искусственные иммунные сети [5].

В работе показано, что на базе искусственных иммунных сетей возможно построение преобразователей биометрия—код, которые не компрометируют биометрический образ и ключ (пароль) субъекта. Для защиты данных пользователя от компрометации можно применить механизм защиты, который состоит в том, что параметры детекторов (вычислительных элементов искусственной иммунной сети) шифруют на ключе, зависящем от откликов других детекторов. Все детекторы выстраивают в цепочку, где каждый последующий детектор зашифрован на выходах предыдущих детекторов. При поступлении на вход зашифрованной иммунной сети биометрического образа "свой" такая сеть может самостоятельно расшифровать детекторы и выработать корректный ключ или пароль пользователя (с определенной долей ошибок). При поступлении образа "чужой" сеть выдаст почти случайный нестабильный код, не соответствующий ключу пользователя.

Описанные техники можно использовать как основу для построения систем защищенного исполнения искусственного интеллекта. Однако для этого необходимо провести дополнительные исследования, направленные на разработку усовершенствованных моделей искусственных иммунных сетей, способных решать задачи кластеризации и регрессии в защищенном исполнении. Кроме того, может потребоваться модернизация алгоритмов их обучения.

Работа выполнена при финансовой поддержке РФФИ (грант № 18-37-00399).

Литература

1. *Mishra P. K., Bhusry M.* Artificial Immune System: State of the Art Approach // International J. Computer Applications. 2015. V. 20. № 120. P. 25—32. DOI: 10.5120/21344-4357.
2. *Vasilyev V. I.* Structural design of shallow neural networks on the basis of minimal complexity principle: Control and Automation (MED), 2016 24th Mediterranean Conference. 2016. DOI: 10.1109/MED.2016.7535872.
3. *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. — 144 с.
4. *Сулавко А. Е.* Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. 2020. Т. 44. № 1. С. 82—91. DOI: 10.18287/2412-6179-CO-567.
5. *Сулавко А. Е., Шалина Е. В.* Биометрическая аутентификация пользователей информационных систем по клавиатурному почерку на основе иммунных сетевых алгоритмов // Прикладная информатика. 2019. № 3 (81). С. 39—53.
6. *Иванов А. И.* Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей. — Пенза, 2014. — 57 с.
7. *Иванов А. И., Чернов П. С.* Протоколы биометрико-криптографического рукопожатия // Системы безопасности. 2018. № 6. С. 2—7.
8. *Dodis Y., Reyzin L., Smith A.* Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // In EuroCrypt. 2004. P. 523—540.
9. *Hao F., Anderson R., Daugman J.* Crypto with Biometrics Effectively // IEEE Transactions on Computers. 2006. V. 55. № 9. P. 1081—1088.
10. *Adamovic S., Milosavljevic M., Veinovic M., Sarac M., Jevremovic A.* Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics // IET Biometrics. 2017. V. 6. № 2. P. 89—96. DOI: 10.1049/iet-bmt.2016.0061.
11. *Lozhnikov P. S., Sulavko A. E., Volkov D. A.* Usage of fuzzy extractors in a handwritten-signature based technology of protecting a hybrid document management system: 2016 10th International Conference on Application of Information and Communication Technologies (AICT), 12—14 October, 2016. — Baku: Azerbaijan, 2016. P. 395—400. DOI:10.1109/ICAICT.2016.7991728.
12. *Сулавко А. Е., Еременко А. В., Борисов Р. В.* Генерация криптографических ключей на основе голосовых сообщений // Прикладная информатика. 2016. № 5. С. 76—89.
13. *Иванов А. И., Сомкин С. А., Андреев Д. Ю., Малыгина Е. А.* О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных "нечетких экстракторов" при их защите наложением гаммы // Вестник УрФО. Безопасность в информационной сфере. 2014. № 2 (12). С. 16—23.
14. *Ложников П. С.* Биометрическая защита гибридного документооборота. — Новосибирск: Изд-во СО РАН, 2017. — 130 с.
15. *Николенко С., Кадурин А., Архангельская Е.* Глубокое обучение. Погружение в мир нейронных сетей. — СПб: Питер, 2018. — 480 с.
16. *Сулавко А. Е., Шалина Е. В., Стадников Д. Г., Чобан А. Г.* Иммунные алгоритмы распознавания образов и их применение в биометрических системах (Обзор) // Вопросы защиты информации. 2019. № 1. С. 38—46.

Artificial intelligence in a secure execution based on immune network models of pattern recognition using biometrics-code converters as an example

E. V. Shalina
Omsk State Transport University, Omsk, Russia

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

In this work, it is shown that, based on the models of artificial immune networks proposed by the authors, it is potentially possible to build AI systems with similar properties. The work does not consider all AI tasks, but only a narrow range of tasks related to biometric identification and authentication.

Keywords: keyboard handwriting, signature, face image, neural networks, classifier committees, machine learning, secure neural network containers.

Biography — 16 references. *Received Match 18, 2020*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26

Постквантовая схема цифровой подписи с двойным маскированием операции экспоненцирования

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский государственный электротехнический университет "ЛЭТИ",
Санкт-Петербург, Россия

А. А. Молдовян, д-р техн. наук*; А. А. Костина*
Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, Россия

Предложен новый способ построения и реализации постквантовой схемы электронной цифровой подписи на основе скрытой задачи дискретного логарифмирования, заданной в конечной некоммутативной ассоциативной алгебре с глобальной двухсторонней единицей. Способ отличается использованием маскирующих операций двух типов, каждая из которых является взаимно коммутативной с базовой операцией экспоненцирования в циклической группе, генерируемой необратимым элементом алгебры, имеющим простое значение локального порядка. В описанной частной реализации криптосхемы в качестве алгебраического носителя применена четырехмерная конечная ассоциативная алгебра с множествами локальных левосторонних и правосторонних единиц, задаваемых в аналитическом виде в зависимости от координат необратимого вектора.

Ключевые слова: защита информации, криптография, электронная цифровая подпись, задача дискретного логарифмирования, конечная ассоциативная алгебра, некоммутативная алгебра, глобальная единица, локальная единица, односторонняя единица.

Ожидаемое появление в ближайшем будущем многокубитового квантового вычислителя обусловливает высокую степень актуальности разработки практичных постквантовых алгоритмов и протоколов с открытым ключом [1—3]. Широко используемые криптографические алгоритмы и протоколы с открытым ключом, основанные на хорошо изученных и апробированных вычислительно-сложных задачах дискретного логарифмирования (ЗДЛ) и факторизации (ЗФ), должны быть заменены в постквантовую эпоху на двухключевые криптосхемы, основанные на вычислительно трудных задачах других типов, а именно на задачах, решение которых на квантовом вычислителе потребует сверхполиномиального времени. Уязвимость к квантовым атакам криптосхем, основанных на вычислительной сложности ЗДЛ и ЗФ, связана с потенциальной возможностью их решения на квантовом вычислителе за полиномиальное время [4—6]. Полиномиальные алгоритмы решения ЗДЛ и ЗФ реализуют сведение каждой из этих двух задач к задаче нахождения длины периода периодической функции, задаваемой по их параметрам. При решении ЗДЛ на квантовом вычислителе формируется периодическая функция, принимающая значения в циклической группе, в которой задана ЗДЛ, и содержащая период с длиной, определяемой значением дискретного логарифма [4—6].

Общим подходом к разработке двухключевых постквантовых криптографических алгоритмов и протоколов является использование в качестве базового криптографического примитива вычислительно-сложных задач, отличающихся от ЗДЛ и ЗФ [7]. Одной из таких задач является скрытая задача дискретного логарифмирования (СЗДЛ) [8]. В качестве алгебраических носителей криптосхем, основанных на СЗДЛ, обычно применяют конечные некоммутативные ассоциативные алгебры (КНАА) различных типов [9, 10].

Использование СЗДЛ как базового постквантового криптографического примитива обосновано тем, что периодические функции, формируемые по открытым параметрам криптосхем и открытым ключам, принимают значения из многочисленных разных групп, содержащихся в алгебраическом

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru
Молдовян Александр Андреевич, профессор, главный научный сотрудник.
E-mail: maa1305@yandex.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anna1805@mail.ru

Статья поступила в редакцию 19 января 2020 г.

носителе, тогда как известные квантовые алгоритмы нахождения длины периодов основаны на способности квантового вычислителя с высокой эффективностью выполнять дискретное преобразование Фурье для случая периодической функции со значениями, лежащими в одной конечной группе [11, 12].

В работах [13, 14] были предложены алгоритмы открытого распределения ключей, открытого и коммутативного шифрования, основанные на СЗДЛ в конечной алгебре кватернионов, заданной над полем $GF(p)$. В работах [15, 16] предложено задавать СЗДЛ в циклической группе, генерируемой необратимым элементом КНАА с глобальной двухсторонней единицей, в качестве общего метода обеспечения защищенности от атак, основанных на сведении СЗДЛ к обычной ЗДЛ в конечном поле $GF(p)$. В работах [17—19] предложены способы сведения СЗДЛ в конечной алгебре кватернионов к обычной ЗДЛ в конечном поле $GF(p^2)$ и поставлена задача поиска новых алгебраических носителей СЗДЛ.

Авторы предлагают способ построения двухключевой схемы электронной цифровой подписи (ЭЦП) с использованием усиленного маскирования операции экспоненцирования в базовой циклической группе, реализуемого с помощью двух различных операций маскирования, являющихся взаимно коммутативными с операцией возведения в степень. Реализация такой возможности обеспечивается использованием необратимого элемента КНАА в качестве генератора базовой циклической группы, элементам которой соответствуют большие множества локальных правосторонних, левосторонних и двухсторонних единиц. Для упрощения процедуры генерации параметров криптосхемы в качестве алгебраического носителя применена четырехмерная КНАА, для которой указанные множества единиц могут быть описаны в виде компактной математической формулы.

Механизмы маскирования и СЗДЛ

Обычно ЗДЛ формулируют следующим образом: задают открытый ключ Y' в виде элемента конечной циклической группы, вычисленного в соответствии с выражением

$$Y' = G^x,$$

где G — генератор циклической группы, имеющей простое значение порядка q;

x — личный секретный ключ ($x < q$).

Нахождение значения x по известным элементам G и Y' называют ЗДЛ. В ряде типов конечных циклических групп (в подгруппах мультипликативной группы простого конечного поля $GF(p)$, в группе точек эллиптической кривой, заданной над конечным полем, и т. д.) для традиционного компьютера известны только сверхполиномиальные алгоритмы решения ЗДЛ. Поэтому при значениях простого порядка q, имеющего большую длину (более 256 бит в случае группы точек эллиптической кривой и более 2048 бит в случае мультипликативной группы простого поля) решение ЗДЛ при использовании обычных компьютеров является практически невыполнимой задачей, т. е. криптосхемы, основанные на ЗДЛ, при соответствующем выборе длины параметров обладают достаточной стойкостью до момента создания многокубитового квантового вычислителя.

Известный квантовый алгоритм решения ЗДЛ основан на задании периодической функции вида $f(i, j) = Y'^{i}G^{j}$, аргументом которой является пара целых чисел i и j. При этом данная функция принимает значения в рассматриваемой конечной циклической группе и содержит период, длина которого зависит от неизвестного значения x, а именно равна $(-1, x)$. Действительно, имеем $Y'^{i}G^{j} = Y'^{i-1}G^{j+x} \Rightarrow f(i, j) = f(i-1, j+x)$. Для функции $f(i, j)$ гипотетический квантовый вычислитель позволяет за полиномиальное время найти длину периода $(-1, x)$, а значит, и значение дискретного логарифма x.

В работах [20—22] предложены схемы ЭЦП, основанные на вычислительной сложности СЗДЛ в КНАА различных типов, имеющих размерность $m = 4$ или 6. В указанных схемах ЭЦП открытый ключ формируют следующим образом. Задают генератор N циклической группы простого порядка q, являющийся элементом личного секретного ключа пользователя, выбирают случайное секретное число x и вычисляют элемент группы N^x. После этого генерируют секретные параметры маскирующих операций ψ_1 и ψ_2 и вычисляют значения $Y = \psi_1(N^x)$ и $Z = \psi_2(N)$, которые лежат вне базовой циклической группы, порождаемой всевозможными степенями генератора N. Из-за того что для корректности работы схемы ЭЦП в качестве операций ψ_1 и ψ_2 выбирают пару "согласованных" маскирующих операций, каждая из которых является взаимно коммутативной с операцией экспоненцирования, функция $f(i,j) = Y^{i}Z^{j}$ содержит период длины $(-1, x)$. Однако она принимает значения, которые лежат в достаточно большом числе различных групп, содержащихся в КНАА, используемом в качестве алгебраического носителя схемы ЭЦП. Благодаря последнему обстоятельству

обеспечивается стойкость к квантовым атакам, основанным на известных алгоритмах нахождения длины периода.

Усиленная маскировка базовой циклической группы может быть достигнута выполнением двух разных маскирующих операций над каждым из элементов N и N^x. Такая возможность возникает при использовании в качестве генератора базовой циклической группы необратимого элемента КНАА, в котором содержится глобальная двухсторонняя единица. В данной работе рассмотрен разработанный способ построения схем ЭЦП, основанных на СЗДЛ с усиленной маскировкой базовой циклической группы. Для упрощения генерации параметров криптосхемы в качестве алгебраического носителя криптосхемы выбрана четырехмерная КНАА, для которой могут быть выведены компактные математические формулы, описывающие множества локальных единиц различных типов, действующих на множестве элементов базовой циклической группы.

Алгебраический носитель схемы ЭЦП

В качестве алгебраического носителя разработанной схемы ЭЦП использована заданная над полем $GF(p)$ четырехмерная КНАА, в которой операция векторного умножения определена с помощью таблицы умножения базисных векторов (ТУБВ).

Задание векторного умножения четырехмерной КНАА, используемой в качестве алгебраического носителя и содержащей глобальную единицу ($\mu^{-1}, \lambda^{-1}, 0, 0$), где $\mu \neq 0, \lambda \neq 0$

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

Операцию умножения двух 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 $\mathbf{A} \circ \mathbf{B} = \sum_{i=0}^{3} \sum_{i=0}^{3} a_i b_j \left(\mathbf{e}_i \circ \mathbf{e}_j\right)$, где вместо произведения всевозможных пар базисных векторов подставляют некоторый базисный вектор или однокомпонентный вектор, указанный в ячейке на пересечении i-й строки и j-го столбца таблицы. Скалярное умножение вектора $\mathbf{A}$ на элемент λ поля $GF(p)$ осуществляют по формуле $\lambda\mathbf{A} = (\lambda a_0, \lambda a_1, \lambda a_2, \lambda a_3)$, т. е. как λ-кратное сложение каждой координаты вектора $\mathbf{A}$.

При задании различных форм СЗДЛ используют единичные элементы нескольких различных типов, содержащихся в КНАА, используемых в качестве алгебраических носителей разрабатываемых криптосхем. Рассматриваемая алгебра выбрана по двум причинам: она содержит глобальную двухстороннюю единицу (это задает существование локальных единиц различных типов, действующих на подмножествах множества необратимых элементов алгебры) и в половине ячеек ТУБВ присутствует структурный коэффициент с нулевым значением, благодаря чему существенно снижается сложность операции векторного умножения. Для вывода формул, описывающих значения единиц, действующих в алгебре, 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;

$\mathbf{X} = (x_0, x_1, x_2, x_3)$ — неизвестный вектор.

Векторное уравнение (1) сводится к следующей паре систем из двух линейных уравнений с двумя неизвестными (x_0, x_3 и x_1, x_2 соответственно):

$$\begin{cases} \mu x_0 a_0 + \lambda x_3 a_2 = a_0; \\ \mu x_0 a_3 + \lambda x_3 a_1 = a_3, \end{cases} \quad (3)$$

$$\begin{cases} \lambda x_1 a_1 + \mu x_2 a_3 = a_1; \\ \lambda x_1 a_2 + \mu x_2 n_0 = n_2. \end{cases} \quad (4)$$

Главный определитель системы (3) равен $\Delta^{(3)} = \mu\lambda(a_0 a_1 - a_2 a_3)$, и для векторов $\mathbf{A}$, координаты которых удовлетворяют условию $a_0 a_1 \neq a_2 a_3$, существует единственное решение: $x_0 = \mu^{-1}$ и $x_3 = 0$. Главный определитель системы (4) равен $\Delta^{(4)} = \mu\lambda(a_0 a_1 - a_2 a_3)$, и для векторов $\mathbf{A}$, координаты которых удовлетворяют условию $a_0 a_1 \neq a_2 a_3$, существует единственное решение: $x_1 = \lambda^{-1}$ и $x_2 = 0$.

Векторное уравнение (2) сводится к следующей паре систем из двух линейных уравнений с двумя неизвестными (x_0, x_2 и x_1, x_3 соответственно):

$$\begin{cases} \mu x_0 a_0 + \lambda x_2 a_3 = a_0; \\ \mu x_0 a_2 + \lambda x_2 a_1 = a_2, \end{cases} \quad (5)$$

$$\begin{cases} \lambda x_1 a_1 + \mu x_3 a_2 = a_1; \\ \lambda x_1 a_3 + \mu x_3 a_0 = a_3. \end{cases} \quad (6)$$

Главный определитель системы (5) равен $\Delta^{(5)} = \mu\lambda(a_0 a_1 - a_2 a_3)$, и для векторов $\mathbf{A}$, координаты которых удовлетворяют условию $a_0 a_1 \neq a_2 a_3$, существует единственное решение: $x_0 = \mu^{-1}$ и $x_2 = 0$. Главный определитель системы (6) равен $\Delta^{(6)} = \mu\lambda(a_0 a_1 - a_2 a_3)$, и для векторов $\mathbf{A}$, координаты которых удовлетворяют условию $a_0 a_1 \neq a_2 a_3$, существует единственное решение: $x_1 = \lambda^{-1}$ и $x_3 = 0$.

Таким образом, существует преобладающее множество векторов, удовлетворяющих условию $a_0a_1 \neq a_2a_3$, для которых векторные уравнения (1) и (2) имеют единственное решение: $\mathbf{E} = (\mu^{-1}, \lambda^{-1}, 0, 0)$. Легко проверить, что значение $\mathbf{X} = \mathbf{E}$ удовлетворяет уравнениям (1) и (2) при всех возможных значениях **A**, однако в случае $a_0a_1 = a_2a_3$ существует много других решений. Вектор **E** будем называть глобальной двухсторонней единицей, а векторы, удовлетворяющие условию $a_0a_1 \neq a_2a_3$, — обратимыми векторами, поскольку для них векторные уравнения

$$\mathbf{X} \circ \mathbf{A} = \mathbf{E}; \quad (7)$$

$$\mathbf{A} \circ \mathbf{X} = \mathbf{E} \quad (8)$$

имеют одно и то же единственное решение: $\mathbf{X} = \mathbf{A}^{-1}$, которое будем называть обратным вектором по отношению к вектору **A**. Для векторов **A**, удовлетворяющих условию $a_0a_1 = a_2a_3$, уравнения (5) и (6) не имеют решений, поэтому эти векторы будем называть необратимыми. Из указанного условия необратимости вектора легко подсчитать число необратимых векторов, равное $p^3 + p^2 - p$. Вычитая число необратимых векторов из числа всех возможных четырехмерных векторов, равного p^4, получим число всех обратимых векторов Ω – порядок мультипликативной группы рассматриваемой алгебры:

$$\Omega = p(p-1)(p^2-1). \quad (9)$$

Произвольный обратимый вектор $\mathbf{V} = (v_0, v_1, v_2, v_3)$ задает некоторую операцию автоморфного отображения (алгебры с глобальной двухсторонней единицей), выражаемую следующей формулой:

$$\varphi(\mathbf{X}) = \mathbf{V} \circ \mathbf{X} \circ \mathbf{V}^{-1}, \quad (10)$$

где переменная **X** пробегает все значения КНАА с глобальной двухсторонней единицей. Легко показать, что операция, задаваемая формулой (10), действительно реализует автоморфное отображение алгебры, а значит, она является взаимно коммутативной с операцией возведения в степень и может быть использована в качестве маскирующей операции при задании СЗДЛ.

Локальные единицы и их типы

Как уже отмечалось, векторные уравнения (1) и (2) имеют много различных решений для необратимых векторов **A**. Эти решения представляют собой локальные единицы, поскольку они действуют как единицы на ограниченном множестве элементов алгебры. При этом в общем случае они представляют собой односторонние единицы: левосторонние для случая уравнения (1) и правосторонние для случая уравнения (2).

Для вывода формулы, описывающей множество локальных левосторонних единиц, соответствующих некоторому необратимому вектору **A**, следует решить системы уравнений (3) и (4). Главный определитель и оба вспомогательных определителя в каждой из этих систем равны нулю, т. е. в рассматриваемом случае каждая из этих систем включает два линейно зависимых уравнения с двумя неизвестными, поэтому имеет p различных решений.

Из первого уравнения системы (3) получаем

$$x_3 = \frac{a_0}{\lambda a_2}(1 - \mu x_0), \quad x_0 = 0, 1, 2, ..., p-1. \quad (11)$$

Из первого уравнения системы (4) получаем

$$x_2 = \frac{a_1}{\mu a_3}(1 - \lambda x_1), \quad x_1 = 0, 1, 2, ..., p-1. \quad (12)$$

Объединяя решения (11) и (12), получаем следующую формулу, описывающую множество локальных левосторонних единиц $\mathbf{L_A} = (l_0, l_1, l_2, l_3)$ мощностью p^2:

$$\mathbf{L_A} = \left(d,\ h,\ \frac{a_1}{\mu a_3}(1 - \lambda h),\ \frac{a_0}{\lambda a_2}(1 - \mu d) \right), \quad d, h = 0, 1, ..., p-1. \quad (13)$$

Легко понять, что все элементы множества (13) действуют как локальные левосторонние единицы на векторы, равные всевозможным линейным комбинациям всевозможных натуральных степеней необратимого вектора **A**, т. е. в общем случае они действуют на достаточно большом подмножестве необратимых элементов рассматриваемой КНАА. При этом подавляющее большинство этих единиц не входит в множество, на котором они действуют. Действительно, большинство векторов, входящих в множество (13), является обратимым (их число равно $p^2 - p$).

Накладывая условие необратимости на правую часть выражения (13), легко установить, что условие необратимости выполняется при $h = \lambda^{-1} - \mu\lambda^{-1}d$, и получить следующую формулу, описывающую все локальные левосторонние единицы, являющиеся необратимыми векторами:

$$\mathbf{L}'_\mathbf{A} = \left(d,\ \lambda^{-1} - \mu\lambda^{-1}d,\ \frac{a_1}{a_3}d,\ \frac{a_0}{\lambda a_2}(1 - \mu d) \right), \quad d = 0, 1, ..., p-1. \quad (14)$$

Для вывода формулы, описывающей множество локальных правосторонних единиц, соответствующих необратимому вектору **A**, следует решить системы уравнений (5) и (6). Главный определитель и оба вспомогательных определителя в каждой из этих систем равны нулю, т. е. в рассматриваемом случае каждая из систем (5) и (6) включает два линейно зависимых уравнения с двумя неизвестными, поэтому имеет p различных решений.

Из первого уравнения системы (5) получаем

$$x_2 = \frac{a_0}{\lambda a_3}\left(1-\mu x_0\right), \quad x_0 = 0, 1, 2, ..., p-1. \tag{15}$$

Из первого уравнения системы (6) получаем

$$x_3 = \frac{a_1}{\mu a_2}\left(1-\lambda x_1\right), \quad x_1 = 0, 1, 2, ..., p-1. \tag{16}$$

Объединяя решения (15) и (16), получаем следующую формулу, описывающую множество локальных правосторонних единиц $\mathbf{R_A} = (r_0, r_1, r_2, r_3)$ мощностью p^2:

$$\mathbf{R_A} = \left(d,\ h,\ \frac{a_0}{\lambda a_3}\left(1-\mu d\right),\ \frac{a_1}{\mu a_2}\left(1-\lambda h\right)\right), \quad d, h = 0, 1, ..., p-1. \tag{17}$$

Элементы множества (17) действуют как локальные правосторонние единицы на векторы, равные всевозможным линейным комбинациям всевозможных натуральных степеней необратимого вектора **A**. При этом подавляющее большинство этих единиц не входит в множество, на котором они действуют. Множество (17) включает $p^2 - p$ обратимых векторов рассматриваемой алгебры.

Накладывая условие необратимости на правую часть выражения (17), легко установить, что условие необратимости выполняется при $h = \lambda^{-1} - \mu\lambda^{-1}d,$ и получить следующую формулу, описывающую все локальные правосторонние единицы, являющиеся необратимыми векторами:

$$\mathbf{R'_A} = \left(d,\ \lambda^{-1} - \mu\lambda^{-1}d,\ \frac{a_0}{\lambda a_3}\left(1-\mu d\right),\ \frac{a_1}{a_2}d\right), \quad d = 0, 1, ..., p-1. \tag{18}$$

Пересечение множеств (13) и (17) задает следующее множество локальных двухсторонних единиц, задаваемых координатами необратимого вектора **A**:

$$\mathbf{E'_A} = \begin{pmatrix} d,\ \dfrac{\lambda a_1 - \mu a_0 + \mu^2 a_0 d}{\lambda^2 a_1},\ \dfrac{a_0}{\lambda a_3}\left(1-\mu d\right), \\ \dfrac{a_0}{\lambda a_2}\left(1-\mu d\right) \end{pmatrix}, \quad d = 0, 1, ..., p-1. \tag{19}$$

Из (19) видно, что необратимому вектору соответствуют p различных локальных двухсторонних единиц, $p-1$ из которых являются обратимыми векторами.

Пересечение множеств (14) и (18) задает единственную локальную двухстороннюю единицу в множестве (19), являющуюся необратимым вектором:

$$\mathbf{E''_A} = \begin{pmatrix} \dfrac{a_0}{\lambda a_1 + \mu a_0},\ \dfrac{a_1}{\lambda a_1 + \mu a_0}, \\ \dfrac{a_2}{\lambda a_1 + \mu a_0},\ \dfrac{a_3}{\lambda a_1 + \mu a_0} \end{pmatrix}. \tag{20}$$

Необратимый вектор **A**, для которого существует единственная локальная единица $\mathbf{E''_A}$, являющаяся необратимым вектором, называется локально обратимым. Такой вектор генерирует циклическую группу с единицей $\mathbf{E''_A}$, которая может быть вычислена по формуле (20) или по формуле $\mathbf{E''} = \mathbf{A}^{\omega}$, где ω – порядок этой группы (называемый также локальным порядком необратимого вектора **A**).

Операция отображения $\psi(\mathbf{X})$ в множестве всевозможных линейных комбинаций всевозможных степеней необратимого вектора **A**, задаваемая формулой $\psi(\mathbf{X}) = \mathbf{X} \circ \mathbf{L_A}$, где локальная левосторонняя единица $\mathbf{L_A}$ не входит в множество (19), является взаимно коммутативной с операцией возведения в степень. Действительно, легко показать, что имеет место равенство

$$\psi(\mathbf{X}^d) = \mathbf{X}^d \circ \mathbf{L_A} = \left(\mathbf{X} \circ \mathbf{L_A}\right)^d = \left(\psi(\mathbf{X})\right)^d.$$

Аналогичная операция отображения $\psi'(\mathbf{X})$ в множестве всевозможных линейных комбинаций необратимого вектора **A**, задаваемая формулой $\psi'(\mathbf{X}) = \mathbf{R_A} \circ \mathbf{X}$, где локальная правосторонняя единица $\mathbf{R_A}$ не входит в множество (19), является взаимно коммутативной с операцией возведения в степень. Действительно, легко показать, что имеет место равенство

$$\psi'(\mathbf{X}^d) = \mathbf{R_A} \circ \mathbf{X}^d = \left(\mathbf{R_A} \circ \mathbf{X}\right)^d = \left(\psi'(\mathbf{X})\right)^d.$$

Операции ψ и ψ' используют в разработанной схеме ЭЦП как второй тип маскирующих операций, усиливающих маскирующий эффект, вносимый операцией автоморфного отображения φ.

Формирование ключей

В разработанной схеме ЭЦП описанную четырехмерную КНАА задают над простым конечным полем $GF(p)$ с характеристикой $p = 2q + 1$, где q — 256-битовое простое число. Выберем случайное натуральное число $x < q$ и случайный необратимый вектор $\mathbf{N}$, имеющий локальный порядок q. Затем по формулам (13) и (17) сгенерируем случайную локальную левостороннюю единицу $\mathbf{L}$ и случайную локальную правостороннюю единицу $\mathbf{R}$, относящиеся к вектору $\mathbf{N}$, такие, что они являются обратимыми векторами порядка $p - 1$ и выполняются условия $\mathbf{R} \circ \mathbf{N} \neq \mathbf{N} \circ \mathbf{R}$ и $\mathbf{L} \circ \mathbf{N} \neq \mathbf{N} \circ \mathbf{L}$. В качестве параметров маскирующих операций автоморфного отображения выберем два обратимых вектора, $\mathbf{Q}$ и $\mathbf{G}$, порядка $p - 1$, для которых выполнены неравенства $\mathbf{Q} \circ \mathbf{N} \neq \mathbf{N} \circ \mathbf{Q}$ и $\mathbf{G} \circ \mathbf{N} \neq \mathbf{N} \circ \mathbf{G}$. Все перечисленные параметры являются секретными и не используются для выполнения процедуры проверки подлинности ЭЦП. Их используют для вычисления открытого ключа.

Открытый ключ генерируют в виде тройки векторов $\mathbf{Y}$, $\mathbf{Z}$ и $\mathbf{T}$, вычисляемых по следующим формулам:

$$\mathbf{Y} = \mathbf{Q} \circ \mathbf{N}^x \circ \mathbf{L} \circ \mathbf{Q}^{-1};$$
$$\mathbf{Z} = \mathbf{G} \circ \mathbf{R} \circ \mathbf{N} \circ \mathbf{G}^{-1};$$
$$\mathbf{T} = \mathbf{Q} \circ \mathbf{L}^{-1} \circ \mathbf{R}^{-1} \circ \mathbf{G}^{-1}.$$

Вектор $\mathbf{T}$ представляет собой согласующий параметр, обеспечивающий корректность работы схемы ЭЦП. Для генерации подписи к некоторому электронному документу M подписант, являющийся владельцем открытого ключа ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{T}$), использует личный секретный ключ в виде тройки векторов ($\mathbf{Q}$, $\mathbf{N}$, $\mathbf{G}^{-1}$) и числа x. Остальные секретные параметры, использованные для формирования открытого ключа, могут быть уничтожены, поскольку они не нужны для вычисления подписи.

Вычисление и проверка подлинности подписи

Для вычисления ЭЦП к документу M подписант должен выполнить следующие процедуры:

- сгенерировать случайное натуральное число $x < q$ и вычислить вектор $\mathbf{V}$:

$$\mathbf{V} = \mathbf{Q} \circ \mathbf{N}^k \circ \mathbf{G}^{-1};$$

- используя некоторую специфицированную хэш-функцию f_H, вычислить первый элемент ЭЦП в виде числа $e = f_H(M, \mathbf{V})$;
- вычислить второй элемент ЭЦП в виде числа $s = k - ex \bmod q$.

Проверку подлинности ЭЦП осуществляют с использованием открытого ключа ($\mathbf{Y}$, $\mathbf{Z}$, $\mathbf{T}$) в соответствии со следующими процедурами:

- вычислить вектор $\tilde{\mathbf{V}}$:

$$\tilde{\mathbf{V}} = \mathbf{Y}^e \circ \mathbf{T} \circ \mathbf{Z}^s;$$

- вычислить значение $\tilde{e} = f_H\left(M, \tilde{\mathbf{V}}\right)$;
- проверить выполнимость равенства $\tilde{e} = e$.

Если равенство выполнено, то подпись признают подлинной, если нет — подпись отвергают.

Для доказательства корректности предложенной схемы ЭЦП предположим, что на вход процедуры проверки подлинности ЭЦП подается подпись (e, s), которая вычислена с использованием правильного личного секретного ключа в соответствии с процедурой генерации подписи. На первом шаге проверочной процедуры вычисляется вектор

$$\tilde{\mathbf{V}} = \mathbf{Y}^e \circ \mathbf{T} \circ \mathbf{Z}^s = \left(\mathbf{Q} \circ \mathbf{N}^x \circ \mathbf{L} \circ \mathbf{Q}^{-1}\right)^e \circ (\mathbf{T}) \circ$$
$$\circ \left(\mathbf{G} \circ \mathbf{R} \circ \mathbf{N} \circ \mathbf{G}^{-1}\right)^s = \mathbf{Q} \circ \left(\mathbf{N}^x \circ \mathbf{L}\right)^e \circ \mathbf{Q}^{-1} \circ$$
$$\circ \left(\mathbf{Q} \circ \mathbf{L}^{-1} \circ \mathbf{R}^{-1} \circ \mathbf{G}^{-1}\right) \circ \mathbf{G} \circ \left(\mathbf{R} \circ \mathbf{N}\right)^s \circ \mathbf{G}^{-1} =$$
$$= \mathbf{Q} \circ \mathbf{N}^{xe} \circ \mathbf{L} \circ \mathbf{Q}^{-1} \circ \mathbf{Q} \circ \mathbf{L}^{-1} \circ \mathbf{R}^{-1} \circ \mathbf{G}^{-1} \circ$$
$$\circ \mathbf{G} \circ \mathbf{R} \circ \mathbf{N}^s \circ \mathbf{G}^{-1} = \mathbf{Q} \circ \mathbf{N}^{xe} \circ \mathbf{N}^{k-ex} \circ \mathbf{G}^{-1} =$$
$$= \mathbf{Q} \circ \mathbf{N}^k \circ \mathbf{G}^{-1} = \mathbf{V},$$

для которого выполнено равенство, подтверждающее подлинность подписи:

$$\tilde{e} = f_H\left(M, \tilde{\mathbf{V}}\right) = f_H\left(M, \mathbf{V}\right) = e.$$

Рассмотренная схема ЭЦП может быть использована в качестве прототипа для разработки других конкретных реализаций предложенного способа с использованием четырехмерных КНАА других типов и шестимерных конечных алгебр. При использовании шестимерных КНАА с глобальной двухсторонней единицей получение формул, описывающих множества локальных односторонних единиц, становится проблематичным. Однако для формирования открытого ключа можно применить алгоритмический способ генерации локальных односторонних единиц. Также представляет интерес поиск шестимерных КНАА с "прореженной" ТУБВ, для которых могут быть получены указанные формулы.

Заключение

Предложен новый способ построения постквантовых схем ЭЦП, основанных на СЗДЛ, отличающийся использованием двух маскирующих операций, выполняемых над каждым из двух элементов базовой циклической группы, применяемых для вычисления элементов открытого ключа. В способе используется наличие большого множества локальных единиц, действующих на множестве элементов циклической группы, генерируемой необратимым элементом алгебры с глобальной двухсторонней единицей, выступающей в качестве алгебраического носителя криптосхемы. Для разработки конкретной схемы ЭЦП, реализующей данный способ, выбрана КНАА с прореженной ТУБВ и получены формулы, описывающие множества локальных правосторонних и левосторонних единиц, используемых для формирования открытого ключа.

В качестве альтернативных алгебраических носителей предложенной постквантовой схемы ЭЦП могут быть непосредственно использованы и другие четырехмерные КНАА [23, 24] с глобальной двухсторонней единицей, для которых получены формулы, описывающие множества локальных единиц.

Литература

1. Post-Quantum Cryptography: Proc. 8th International Conference, PQCrypto 2017. Utrecht, The Netherlands, June 26—28, 2017. Lecture Notes in Computer Science series. — Springer, 2017. V. 10346.
2. Post-Quantum Cryptography: Proc. 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9—11, 2018. Lecture Notes in Computer Science series. — Springer, 2018. V. 10786.
3. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. URL: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf
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 Attacks on Public-Key Cryptosystems. — Springer, 2014. — 207 p.
6. *Smolin J. A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. V. 499. № 7457. P. 163—165.
7. Post-Quantum Cryptography: Proc. 10th International Conference, PQCrypto 2019, Chongqing, China, May 8—10, 2019. — Lecture Notes in Computer Science, 2019. V. 11505. — 420 p.
8. *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.
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. *Moldovyan D. N.* Non-Commutative Finite Groups as Primitive of Public-Key Cryptoschemes // Quasigroups and Related Systems. 2010. V. 18. P. 165—176.
14. *Moldovyan D. N., Moldovyan N. A.* Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms // Quasigroups and Related Systems. 2010. V. 18. P. 177—186.
15. *Moldovyan D. N., Moldovyan N. A.* A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols: Proc. 5th Int. Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ANCS. 2010. St. Petersburg, September 8—11, 2010. Lecture Notes Comp. Sci. — Springer Verlag, 2010. V. 6258. P. 183—194.
16. *Горячев А. А., Молдовян Д. Н., Куприянов И. А.* Выбор параметров задачи скрытого дискретного логарифмирования для синтеза криптосхем // Вопросы защиты информации. 2011. № 1. С. 19—23.
17. *Глухов М. М.* К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 5—22.
18. *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.
19. *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.
20. *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.
21. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
22. *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.
23. *Абросимов И. К., Ковалева И. В., Молдовян Н. А.* Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3—13.
24. *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 Signature Scheme with Double Masking of the Exponentiation Operation

D. N. Moldovyan
St. Petersburg Institute for Informatics and Automation of State Electrotechnical University "LETI", St. Petersburg, Russia

A. A. Moldovyan, A. A. Kostina
St. Petersburg Institute for Informatics and Automation the RAS, St. Petersburg, Russia

A new method for designing the signature schemes based on the hidden discrete logarithm problem and its implementation are 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 masking operations of different types each of which is mutually commutative with the basic exponentiation operation in a cyclic group generated by a non-invertible element of the algebra, which has sufficiently large prime order. In a particular implementation of the method the 4-dimensional finite algebra, containing large sets of the local left-sided and right-sided units described by mathematical formulas is used as the algebraic support of the signature scheme.

Keywords: information protection, cryptography, digital signature, discrete logarithm problem, finite associative algebra, non-commutative algebra, global unit, local unit, single-sided unit.

Bibliography 24 references. *Received January 19, 2020*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.05

Анализ существующих методик оценки защищенности информационных систем

В. И. Петренко, канд. техн. наук; *А. В. Шерстобитов*
ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, Россия

Проведен сравнительный анализ методик оценки защищенности информационных систем. Рассмотрены слабые и сильные стороны наиболее известных подходов к ее оценке. Использование результатов данного исследования позволит в дальнейшем усовершенствовать наиболее оптимальный метод оценивания защищенности информационных систем.

Ключевые слова: информационная система, защищенность, методы оценки, информационная безопасность.

Темпы глобализации, повсеместное увеличение баз данных, развитие информационно-коммуникационных систем, содержащих конфиденциальную информацию о гражданах, доказывают актуальность задачи обеспечения защиты информации, циркулирующей в центрах хранения и обработки данных (ЦХОД; также часто в литературе встречаются такие определения, как центр обработки данных (ЦОД) или дата-центр).

Почти вся информация, обрабатываемая в информационных системах ЦХОД, является конфиденциальной, ее требуется надлежащим образом защищать, поскольку постоянно увеличивается количество взломов сайтов, начиная от интернет-магазинов и заканчивая сайтами крупных фирм и даже правительственных ресурсов. DDoS-атаке подвергается все большее число банковских структур. По данным аналитиков компании Positive Technologies, за первые три квартала 2019 г. зафиксировано 167 атак на госучреждения (за такой же период в 2018 г. зафиксировано 133 атаки) [1]. За 8 месяцев 2019 г. правоохранительные органы выявили 180 153 (+66,8 % по сравнению с 2018 г.) преступления, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, о чем сообщает Генпрокуратура на своем сайте [2]. Тенденция к увеличению масштабов и мощностей атак не может не настораживать.

Учитывая изложенное, можно заключить, что необходимо совершенствовать существующие средства защиты информации. Одна из серьезных трудностей обеспечения защищенности информации — это отсутствие единой для всех информационных систем (ИС) системы оценки защищенности информации, позволяющей дать достоверную, недвусмысленную оценку уровня защиты.

Для разработки универсальной оценки защищенности информации необходимо провести анализ существующих методик оценки, чтобы выявить их плюсы и минусы, учитывая состояние развития информационных технологий.

Постановка задачи

Защищенность информационных и программных ресурсов ИС складывается из обеспечения ее основных свойств: целостности, доступности и конфиденциальности [3]. Оценка защищенности позволяет достичь определенного уровня уверенности в том, что функциональные возможности безопасности информационных сетей, а также меры доверия, предпринятые по отношению к ним, отвечают предъявленным требованиям.

По своей сути оценка защищенности является комплексной. Она характеризует защищенность информации и поддерживающей инфраструктуры от совокупности угроз на всех стадиях жизненного цикла информационной системы.

Петренко Вячеслав Иванович, директор института информационных технологий и телекоммуникаций, заведующий кафедрой организации и технологии защиты информации.
E-mail: vipetrenko@ncfu.ru
Шерстобитов Антон Владимирович, аспирант.
E-mail: av431994@yandex.ru

Статья поступила в редакцию 24 марта 2020 г.

Существует много различных подходов к оценке защищенности, но все их можно условно разделить на три группы:

- формальные методики (например, модель системы защиты с полным перекрытием) [4—10];
- статистические подходы к оценке защищенности, основанные на учете числа инцидентов безопасности информационных систем [3, 5, 11—14];
- классификационные методики (например, метод оценки защищенности информационной системы по требованиям стандартов информационной безопасности) [15—18].

Рассмотрим каждое из направлений в оценке защищенности подробнее.

Сравнительный анализ методик оценки защищенности информационных систем

В [7, 9] предложена формальная модель оценки защищенности ИС. В этих методиках использовано формальное описание системы защиты ИС, в которой рассматривается взаимодействие угроз безопасности и систем защиты.

Стоит отметить, что в этом вопросе существуют разногласия у разных ученых из-за возникновения сложностей в формализации основных понятий. Чаще всего у каждого автора имеется свое формальное описание ИС (как, например, в [19]).

Наиболее часто используемой моделью для описания информационной системы с точки зрения обеспечения ее безопасности является субъектно-объектная модель, в соответствии с которой ИС делят на множества объектов (пассивных компонентов, служащих для хранения информации, для которых необходимо обеспечить конфиденциальность, целостность и доступность) и субъектов (активных компонентов). Отношения между ними определены множеством операций, которые субъекты могут выполнять. Однако имеется ряд недостатков. Например, отсутствует такой фактор, как ценность информации [13].

В качестве примера формального описания информационной системы обработки данных ЦХОД можно привести следующее. В информационной системе обработки информации можно выделить несколько составляющих подсистем:

- ввода информации;
- обработки информации;
- вывода (визуализации) информации;
- хранения информации;
- защиты информации.

Получаем следующие множества, описывающие информационную систему обработки информации:

- объектов ввода информации $I = \{i_j\}$;
- объектов обработки информации $P = \{p_j\}$;
- вывода (визуализации) информации $O = \{o_j\}$;
- объектов хранения информации $S = \{s_j\}$;
- механизмов защиты информации $M = \{m_j\}$.

Таким образом, имеем пять множеств, элементы которых находятся между собой в определенных отношениях, они то и представляют собой информационную систему. Для наглядного описания используем графовую модель информационной системы (рис. 1).

Как видно из представленной модели, существует множество точек, через которые могут быть реализованы угрозы информационной безопасности на всех элементах ИС.

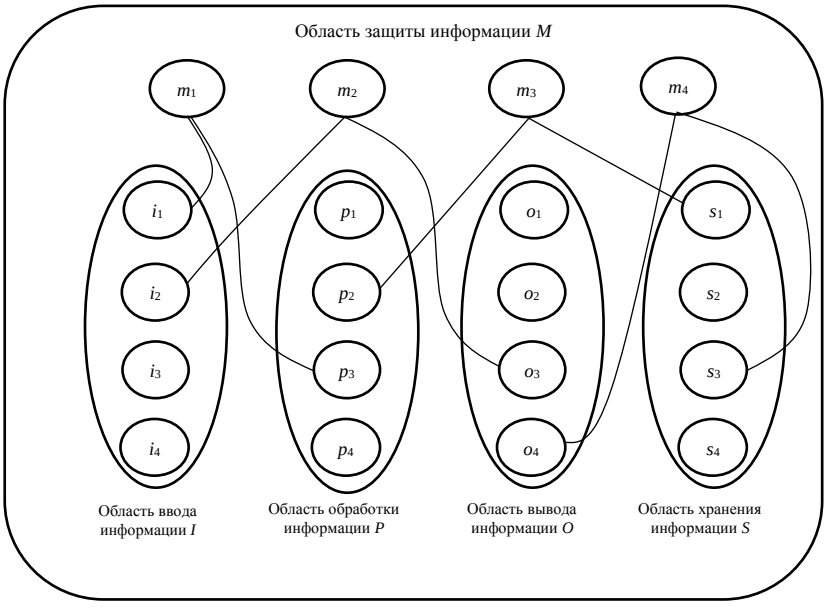


Рис. 1. Модель информационной системы

Чаще всего при проведении формальных методик оценки защищенности используют модель системы защиты с полным перекрытием, в которой рассматривают взаимодействие множеств области угроз ($T = \{t_i\}$), защищаемой области ($O = \{o_j\}$) и системы защиты ($M = \{m_k\}$). Учитывая особенности систем защиты, вводят также еще два элемента:

- V — набор уязвимых мест, определяемый подмножеством декартова произведения $T \cdot O$: $v_r = \langle t_i, o_j \rangle$. Под уязвимостью системы защиты понимают возможность осуществления угрозы t в отношении объекта o;
- B — набор барьеров, определяемый декартовым произведением $V \cdot M$: $b_l = \langle t_i, o_j, m_k \rangle$. Барьеры представляют собой пути осуществления угроз безопасности, перекрытые средствами защиты.

В данном случае уязвимость представляет собой вероятность реализации угрозы t в отношении объекта o, а барьеры олицетворяют перекрытые средствами защиты пути осуществления этих угроз [7].

Таким образом, в конечном счете получаем систему, состоящую из пяти элементов $\langle T, O, M, V, B \rangle$, которая описывает систему защиты, учитывая существующие уязвимости.

Для определения величины защищенности S используем следующую формулу:

$$S = \frac{1}{\sum_{\forall b_k \in B} \left[P_k L_k \left(1 - R_k\right) \right]},$$

где P_k — вероятность появления угрозы;
L_k — величина ущерба при положительном осуществлении угрозы в отношении защищаемых объектов;
R_k — уровень сопротивляемости механизма защиты m_k, характеризуемый вероятностью его преодоления.

В знаменателе определена суммарная величина остаточных рисков, связанных с возможностью осуществления угроз T в отношении объектов защищаемой области O при использовании механизмов защиты M. Данная величина характеризует общую уязвимость системы защиты, а защищенность определена как величина, обратная уязвимости. При отсутствии в системе барьеров, перекрывающих некоторые уязвимости, уровень сопротивляемости механизма защиты принимают за нуль [7, 9].

Смысл подхода состоит в том, что вывод об уровне защищенности делают на основании значения показателя эффективности системы защиты информации.

К достоинствам данной методики можно отнести точную оценку уровня защищенности по заданным угрозам безопасности.

Недостатком является то, что на практике получение точных значений указанных характеристик затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Например, оценку ущерба в результате несанкционированного доступа к информации политического характера точно определить очень сложно.

Таким образом, формальные методики оценки защищенности очень редко применяют в чистом виде. Чаще всего их используют вместе с иными подходами к оценке, например со статистическими.

Базирующиеся на сборе и накоплении статистических данных о частоте возникновения инцидентов в защищаемой системе статистические методики позволяют рассчитать вероятность возникновения угроз, основываясь на накопленной статистике. На рис. 2 продемонстрированы основные этапы данных подходов.

К подобным методикам относят и оценку защищенности при помощи анализа риска информационной безопасности. Она позволяет создать надежную основу для защиты информации в организации. Возможно, данная процедура является одним из самых важных шагов, предпринимаемых организацией для повышения своей безопасности. Это имеет решающее значение для понимания того, где находятся самые большие уязвимости в организации, а также какие потенциальные внешние угрозы могут возникнуть [20, 21].

Суть данной методики заключается в том, чтобы определить численный показатель риска ИБ в целях принятия эффективных мер по защите информации.

Например, в работе [22] оценку степени защищенности осуществляли за счет оценки соответствующих показателей. Главные из них — это риск и степень защищенности.

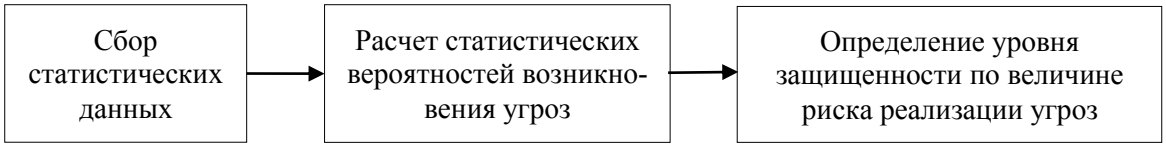


Рис. 2. Основные этапы статистических подходов

Риск определяет вероятность реализации потенциальной угрозы со стороны злоумышленников и причинения ущерба информационному активу или его области объекта информационных технологий через установленные уязвимости системы защиты и безопасности.

Степень защищенности информации представляет собой меру, определяющую возможность предотвращения реализации потенциальной угрозы безопасности посредством применения комплекса средств обеспечения защиты.

Такие методики оценки защищенности позволяют:

- использовать количественные и качественные методы оценки уровня риска и степени защищенности конфиденциальной информации при любых известных априорно количествах характеристик угроз, числе уязвимостей данной системы, количестве средств обеспечения защиты и безопасности информационного актива;
- провести объединение количественных и качественных показателей и критериев в интегральный показатель степени защищенности информации;
- определить уровень ущерба, нанесенного злоумышленником, для любого вида информационного актива или его области объекта информационных технологий по следующему соотношению:

уровень ущерба = уровень риска × *ценность информационного актива*;

- определить показатель степени защищенности информации с помощью следующего соотношения:

показатель степени защищенности = наибольший уровень риска – уровень риска;

- определить уровень ущерба, предотвращенного за счет использования средств обеспечения защиты информационного актива, с использованием соотношения:

уровень предотвращенного ущерба = степень защищенности информации × *ценность информационного актива*.

Все это позволит в полной мере охарактеризовать степень защищенности объекта информационных технологий, чтобы в дальнейшем провести оценку эффективности средств защиты информационных активов.

В [23] рассмотрена модель комплексной оценки защищенности с учетом изъянов в системе безопасности (см. рис. 3).

В данном случае комплексная оценка защищенности предполагает прохождение следующих этапов:

- идентификация и определение ценности объектов защиты;
- формирование перечня угроз и оценка их опасностей (вероятностей) на основе видового дерева;
- формирование перечня системы защиты (базового уровня защиты) с учетом нормативных требований на основе видового дерева;
- вычисление ущерба с учетом применения системы защиты и оценка остаточного риска, как правило в ранговой шкале, на основе экспертной методики оценки возможности реализации угрозы;
- формирование дополнительных мер защиты и системы защиты информации для достижения приемлемого риска.

После обработки данных производят рациональное и комплексное ранжирование угроз для организации. Оно включает как важность активов, находящихся под угрозой, так и широкий спектр возможных непредвиденных обстоятельств. Разумный план безопасности позволит начать устранение выявленных рисков с наивысшими показателями [24].

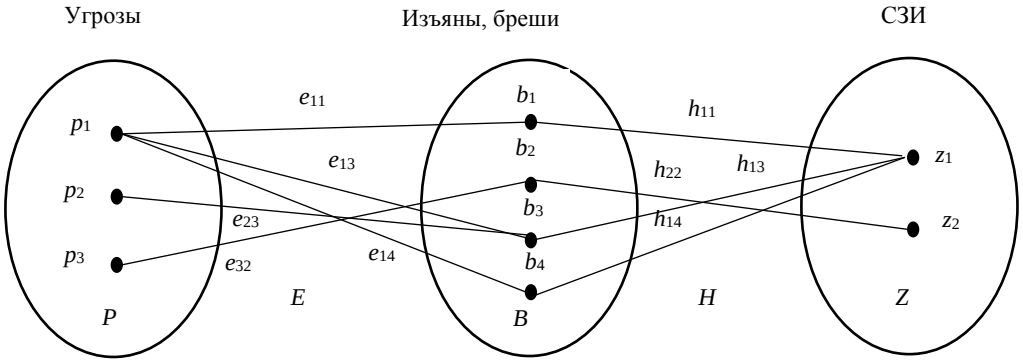


Рис. 3. Модель комплексной оценки защищенности сети с учетом изъянов в системе безопасности

Стоит также упомянуть стоимостный подход к оценке степени защищенности конфиденциальной информации. Он основан на применении стоимостных показателей и критериев, характеризующих стоимость информационного актива, затраты на реализацию защиты сохранности информации, а также затраты на создание и эксплуатацию объектов информационных технологий и средств осуществления защиты.

Одним из главных недостатков такого подхода является отсутствие взаимосвязи между показателями степени защищенности и характеристиками внешних и внутренних факторов, а также свойств объектов информационных технологий, оказывающих влияние на безопасность информационного актива [22].

Некоторые специалисты предлагают проводить оценку защищенности информационной системы, используя теорию игр, а также вероятность реализации угроз информационной безопасности. В [25] рассмотрена игровая модель системы защиты информации, решающая проблемы выбора решения, обеспечивающего оптимальное соотношение между затратами на средства защиты и снижением риска эксплуатации.

При этом стратегии одного игрока (защитника) заключены в приведении автоматизированной системы в соответствие с требованиями определенного класса защищенности. Под классом защищенности понимают определенный набор требований к функциям защиты системы.

Стратегии другого игрока (нарушителя) заключены в реализации угрозы, относящейся к определенному классу угроз.

В методике предполагается, что имеется система информационной безопасности, в которой существует множество уязвимостей $Y = \{y_1, y_2, \ldots, y_i\}$. Имеется нарушитель, который может реализовать множество угроз $T = \{t_1, t_2, \ldots, t_j\}$. В таком случае множество стратегий защиты системы $D = \{d_1, d_2, \ldots, d_j\}$ будет направлено на ликвидацию уязвимостей. Мерой защиты будет сумма затрат на осуществление предлагаемых мер и ожидаемых потерь в случае реализации угрозы.

Функция выигрыша будет представлять собой сумму затрат на реализацию предлагаемых мер защиты и ожидаемых потерь в случае реализации угрозы определенного класса при условии приведения системы в соответствие с требованиями по классу защищенности.

К достоинствам такого метода можно отнести высокую точность при условии полноты входных данных. К недостаткам относят:

- необходимость большого количества входных данных;
- быстрый рост сложности алгоритма;
- большое количество вычислений;
- высокую трудоемкость;
- неточность и субъективность при оценке вероятностей угроз и стоимости информации [25].

Еще один подход к количественному анализу безопасности компьютерных систем представлен в [26, 27], где авторы предлагают новую методологию. Она предполагает возможность количественно оценить интерпретацию того, как действуют нападающие и насколько они предсказуемы. В основе предложенной методологии используют вариант дерева атаки, способный систематически представлять все возможные вредоносные атаки, выполняемые для нарушения безопасности системы. Практическая реализация данной модели направлена на получение количественной оценки сложности нападения.

Достоинством рассмотренных подходов к оценке защищенности статистических методик в некоторых источниках, называемых количественными, является то, что они позволяют создавать сложные математические модели для получения точных результатов.

Однако стоит отметить, что кроме сложных расчетов возникают дополнительные трудности, связанные с тем, что получить реальные данные, используя исключительно статистические подходы, очень сложно. Это обусловлено тем, что довольно тяжело собрать информацию по всем событиям, включая те, вероятность которых чрезвычайно мала. К тому же следует понимать, что любая система не является статичной. Она находится в процессе постоянного развития, при котором могут меняться аппаратная составляющая, программное обеспечение и заменяться средства защиты информации.

В связи с трудностью постоянного сбора актуальной статистической информации в рамках изменяемой защищаемой системы статистические подходы при оценке защищенности применимы лишь частично как дополнительное средство при наличии достоверной статистической базы. Некоторые этапы данных методов можно использовать при составлении таблиц вероятностей реализации наиболее распространенных угроз информации в рамках определенной категории предприятий.

В среде специалистов намного больше распространены классификационные подходы с применением неформальных моделей защиты, в качестве значений показателей объектов которых используют их отнесение к определенным категориям. Используя данную методику, точные показатели защищенности получить невозможно, зато она позволяет классифицировать и провести сравнение информационных систем по уровню защищенности.

К таким подходам принадлежит метод оценки защищенности информационной системы по требованиям стандартов информационной безопасности. Например, в целях оценки комплексности системы защиты информации применяют ГОСТ ИСО/МЭК 15408 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Результат оценки может быть выведен на основе состояния защищенности всех ее комплектующих, существующие уязвимости которых могут привести к потере, искажению, уничтожению информации.

Организационно-правовые меры в качестве элементов управления защитой информации предусматривают стандарты ГОСТ ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" и ГОСТ ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий".

Общая суть рассматриваемого метода заключается в следующем: составляют опросные листы, представляющие собой упорядоченную структуру – простой ориентированный граф, не содержащий циклов. Каждая вершина – это очередной вопрос, имеющий один или несколько вариантов ответа, в соответствии с которыми взвешиваются ребра [18]. Вопросы задают только в случае, если созданы соответствующие условия. В меру непонимания или некомпетентности в какой-либо области некоторые вопросы могут быть пропущены пользователем.

Основные этапы, типичные для данной категории подходов к оценке защищенности, перечислены на рис. 4.

К классификационным подходам также можно отнести метод экспертных оценок, основанный на взаимодействии специалистов (экспертов), на получении и обработке сложившихся мнений экспертов по возникшим вопросам. Экспертные решения формируются в целях подготовки информации для принятия решений об уровне защищенности системы [23, 28].

В качестве основного недостатка здесь можно указать, что существующие методики оценки защищенности информационных систем направлены на определенный стандарт, необдуманное применение которого сопровождается ложным чувством защищенности. Внедрение методики необходимо осуществлять с непременным учетом специфики организации. К тому же существует такая проблема, как несвоевременное обновление национальных стандартов, которое не синхронизируют с пересмотром международных стандартов ISO (например, ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006) [29].

Стоит заметить, что в информационной сфере все чаще используют возможности нейронных сетей. Идет разработка методов оценки защищенности ИС с использованием нейронной сети. Например, в работе [30] рассмотрена оценка защищенности на основе требований стандартов информационной безопасности, основные расчеты в которой проводят благодаря нейронной сети. Иными словами, «обучив» нейронную сеть, начинают проводить оценку защищенности, а в дальнейшем необходимо только загружать новые данные, все остальное сеть сделает сама [30].

В [8, 30—34] оценка защищенности основана на нейронных сетях.

Как отмечено в [8], сети могут автоматически получать и накапливать знания. Важным свойством нейронных сетей при решении прикладных задач является их способность к обучению и к обобщению полученных знаний. Натренированная на ограниченном множестве обучающих выборок сеть обобщает накопленную информацию и вырабатывает ожидаемую реакцию применительно к данным, не обработанным в процессе обучения. Для классификации и распознавания образов сеть обучают важнейшим их признакам. В процессе обучения выделяют признаки, отличающие образы друг от друга, которые и составляют базу для принятия решений об отнесении образов к соответствующим классам [8].

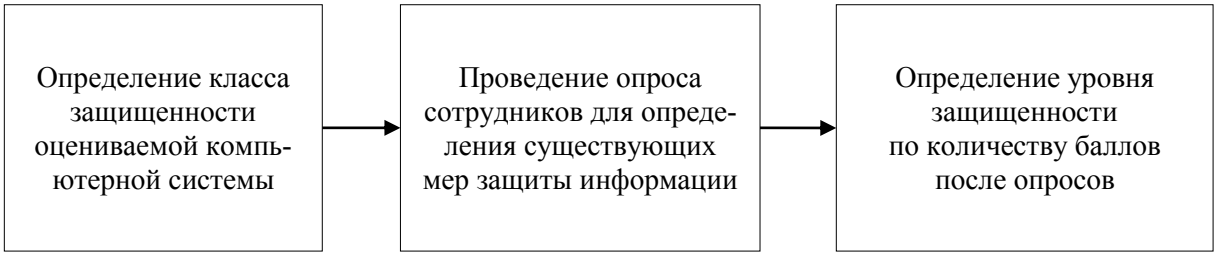


Рис. 4. Основные этапы классификационных подходов

В общем виде алгоритм работы методики оценки защищенности с помощью нейронных сетей состоит из следующих этапов.

- Получение входных данных (исходная информационная система для анализа).
- Анализ входных данных (на основе текущей системы определяют класс автоматизированной системы в соответствии с РД ФСЭТК, определяют требования на основе постановления РФ №1119, которым должна удовлетворять система защиты). Все операции данного этапа основаны на руководящих документах, законах, регламентирующих актах. Все они входят в общую библиотеку документов представленного алгоритма.
- После получения и формирования всех необходимых входных данных формируют параметры для нейронной сети.
- После формирования входных этапов проиизводят запуск нейронной сети. При необходимости проводят обучение нейронной сети, для того чтобы использовать результаты каждого запуска для последующих запусков модели.

В работах [32, 33] представлена модель оценки защищенности, главным параметром которой являются дестабилизирующие факторы, формируемые на основе банка данных ФСТЭК. Эти факторы служат основой в нейронной сети. Они позволяют полнее оценить возможные угрозы исследуемой информационной системы.

Недостатком данной методики является трудоемкость обучения нейронных сетей. Требуется большая база исходных данных. К тому же каждый день появляются новые уязвимости и угрозы для информационных систем.

Также стоит рассмотреть метод, соединяющий в себе методики статистического и классификационного подходов. Применение данного вида оценки позволит получить рекомендации по модернизации системы защиты. Однако на практике реализация полученных после проведения оценки рекомендаций весьма затруднительна, поскольку стандарт не учитывает информацию, собранную анализируемой системой в процессе эксплуатации.

Таким образом, перед специалистом появляется проблема одновременного учета и требований стандарта, и статистики (например, статистических данных по инцидентам информационной безопасности), накопленной в процессе функционирования системы обработки информации.

Логично предположить, что учет всех произошедших инцидентов невозможен из-за большого разнообразия видов событий и их числа. Следовательно, есть необходимость сформировать из числа зафиксированных инцидентов базу прецедентов с использованием алгоритма анализа защищенности. Базу прецедентов собирают из базы инцидентов, которую, в свою очередь, можно сформировать из журналов межсетевых экранов и других средств защиты информации. В основе данного подхода лежит модель оценки защищенности, построенная с применением аппарата нечеткой логики (рис. 5) [5].

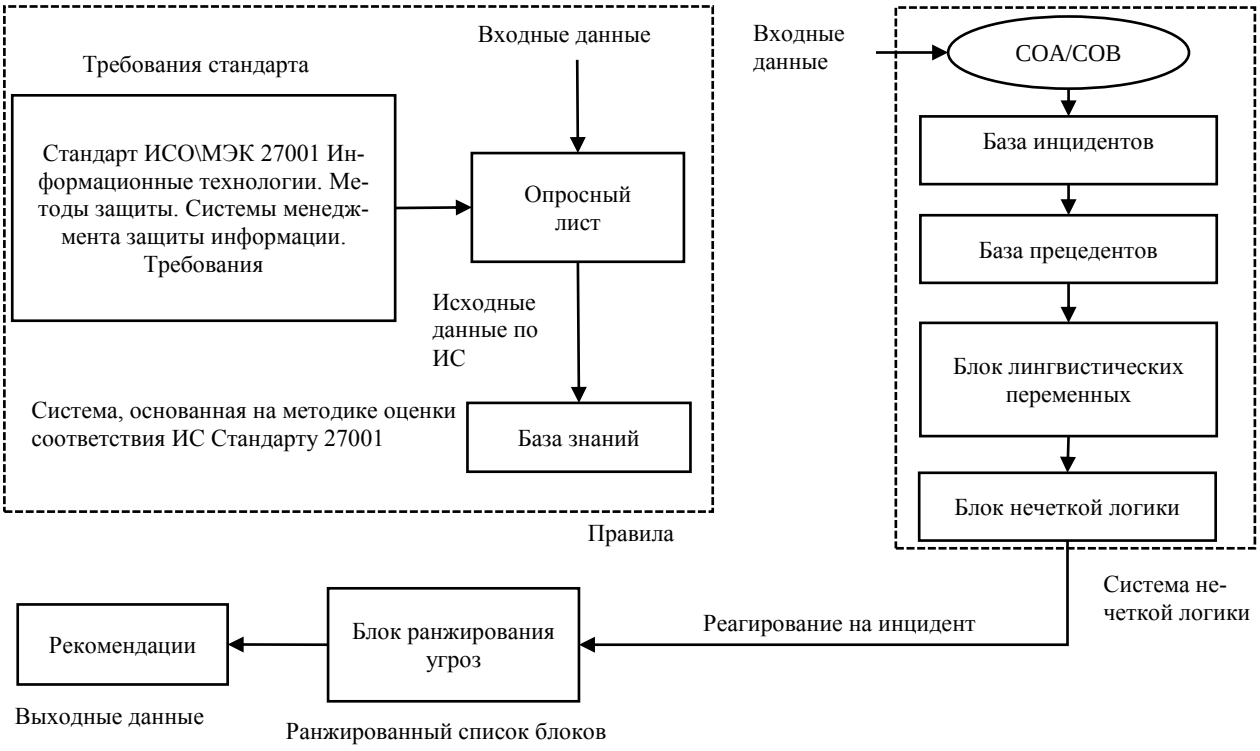


Рис. 5. Схема модели оценки защищенности с применением аппарата нечеткой логики

Однако для корректной работы требуется высокая квалификация пользователя, поскольку необходима предварительная настройка части параметров:

- выбор представления лингвистических переменных;
- определение граничных значений термов.

Кроме перечисленного, все остальное не требует от пользователя действий: на вход системы подают параметры, выбранные для оценивания, а на выходе формируется определенное управляющее воздействие, которое поступает в блок ранжирования угроз, где, в свою очередь, формируется список актуальных угроз, требующих повышенного внимания при создании или модернизации системы. В этом и заключено основное отличие от стандартизированного подхода, выдающего список рекомендаций, сформулированных только на основе сравнения полученных результатов с тем, что требует стандарт [5].

В целом, говоря о недостатках подходов, ориентированных только на сравнение с требованиями стандартов обеспечения информационной безопасности, можно выделить следующие:

- требование высокой квалификации аналитика;
- узкая направленность на определенный стандарт;
- необходимость тестирования и сертификации вычислительной системы в целом.

В качестве заключения можно сказать о том, что наиболее распространены три основных подхода к оценке защищенности (табл. 1):

- формальный; считается наиболее точным по результатам, но сам процесс проведения оценки является очень сложным из-за проблем в формализации основных понятий;
- статистический; базируется на сборе и накоплении статистики об инцидентах в информационных системах и расчете вероятностей угроз безопасности;
- классификационный; не позволяет получить точное значение показателя защищенности, но дает возможность классифицировать и сравнивать информационные системы по уровню защищенности.

Заключение

Для наглядного представления результатов исследования приведем данные критериального сравнительного анализа методов оценки защищенности в виде таблицы (табл. 2).

На основе указанных критериев проведен сравнительный анализ методов оценки защищенности информационных систем (табл. 3).

Таблица 1

Сравнительная таблица методик оценки защищенности

Методики	Описание	Недостатки
Формальные	Решение об уровне защищенности делается на основании значения показателя эффективности системы защиты информации	Внимание уделяется лишь одному из аспектов информационной безопасности – защите информации от несанкционированного доступа
Статистические	Предварительное оценивание двух параметров: вероятности реализации угрозы и потенциального ущерба	Метод требует значительных капиталовложений и времени на изучение всех угроз ради оценивания всего лишь одной категории
Классификационные	Показатели оценки защищенности зависят от эффективности информационной системы. Чем выше эффективность системы в целом, тем выше уровень защищенности	Субъективный фактор в оценке риска и неабсолютная точность

Таблица 2

Критерии оценки метода

Критерий	Содержание
Точность расчетов	Степень объективности полученных результатов
Скорость расчетов	Скорость обработки исходных данных
Трудоемкость расчетов	Затраты вычислительных ресурсов, время работы специалиста
Эффективность применения	Удобство применения метода
Наглядность результатов	Возможность визуализации полученных результатов
Возможность количественной оценки	Возможность формирования числового показателя

Таблица 3

Сравнительный анализ методов оценки защищенности

Методы \ Критерии	Точность расчетов	Скорость расчетов	Трудоемкость расчетов	Эффективность применения	Наглядность результатов	Возможность количественной оценки	Итог
Экспертных оценок	1	1	0,5	0,5	1	0,5	4,5
На основе расчета риска	0,5	1	0,5	0,5	0,5	1	4
С помощью нейронной сети	0,5	0	0	1	1	1	3,5
Комплексная оценка защищенности (формальные методы)	1	0,5	0	0	0,5	1	3
Графовый	0,5	0	0	0	0,5	0,5	1,5

Исходя из полученных данных (см. таблицы) можно сделать заключение, что не все методы подходят для оценки защищенности информационных систем. Сравнительный анализ показал, что метод экспертной оценки и метод оценки защищенности на основе расчета риска реализации угрозы позволяют дать наиболее корректную оценку защищенности ИС.

На основе проведенного анализа можно сделать вывод о том, что не существует единой системы оценки защищенности, подходящей под все условия. Это обстоятельство вынуждает каждый раз подбирать метод оценки защищенности, учитывая специфику защищаемого объекта. Следовательно, назрела необходимость в разработке если не универсального, то относительно гибкого метода оценки защищенности.

Литература

1. Кибербезопасность 2019-2020. Тренды и прогнозы [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ cybersecurity-2019-2020/ (дата обращения: 25.02.2020).
2. Статистические данные о зарегистрированных преступлениях на территории Российской Федерации [Электронный ресурс]. Режим доступа: https://genproc.gov.ru/smi/news/genproc/news-1703326/ (дата обращения: 25.02.2020).
3. *Казарин О. В., Кондаков С. Е., Троицкий И. И.* Подходы к количественной оценке защищенности ресурсов автоматизированных систем // Вопросы кибербезопасности. 2015. № 2 (10). С. 31—35.
4. *Баранова Ж. М., Захарова К. В.* Использование теории графов для создания методики защищенности распределенной вычислительной системы // Проблемы безопасности российского общества. 2016. № 2. С. 159—166.
5. *Жукова М. Н., Коромыслов Н. А.* Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Изв. ЮФУ. Технические науки. 2013. № 12 (149). С. 63—69.
6. *Миков Д. А., Булдакова Т. И., Сюзев В. В., Смирнова Е. В., Бауман Ю. И.* Модели оценки защищенности данных в информационно-управляющих системах реального времени // Проблемы современной науки и образования. 2019. № 11—1 (144). С. 15—20.
7. *Ступина А. А., Золотарев А. В.* Сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем // Вестник Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. 2012. № 4 (44). С. 56—61.
8. *Трапезников Е. В.* Алгоритм модели оценки защищенности информационной системы на основе нейронной сети // Изв. ТулГУ. Технические науки. 2017. № 2. С. 312—318.
9. *Астахов А.* Анализ защищенности корпоративных автоматизированных систем [Электронный ресурс]. Режим доступа: http://iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem (дата обращения: 02.05.2019).
10. *Витенбург Е. А.* Формализованная модель оценки защищенности информационной системы предприятия // Вестник Российского нового университета. Сер. "Сложные системы: модели, анализ и управление". 2019. № 3. С. 92—101.
11. *Белокурова Е. В., Дерканосова А. А., Змеев А. В., Сидельников А. П.* Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем // Вестник Воронежского гос. ун-та инженерных технологий. 2015. № 2. С. 86—91.
12. *Елисеев А. Н., Федоров И. А., Шитов А. Г.* Способ количественной оценки уровня защищенности распределенных информационных систем // Проблемы безопасности российского общества. 2015. № 4. С. 112—118.
13. *Петров С. А., Хорев П. Б.* Применение онтологии при оценке защищенности информационных систем // Вестник МГТУ "Станкин". 2015. № 3 (34). С. 124—128.
14. *Хисамов Ф. Г., Жук А. С., Шерстобитов Р. С.* Математическая модель оценки защищенности информации от несанкционированного доступа при проектировании автоматизированных систем в защищенном исполнении // Изв. ЮФУ. Технические науки. 2017. № 9 (194). С. 91—102.
15. *Бурькова Е. В.* Задача оценки защищенности информационных систем персональных данных // Вестник Чувашского ун-та. 2016. № 1. С. 112—118.
16. *Зюзин А. С.* Современные тенденции оценки защиты информации // Полиматематический сетевой электронный

научный журнал Кубанского гос. аграрного ун-та. 2015. № 107. С. 498—509.

17. *Мангилёва С. А.* Анализ методик оценки защищенности информации в организациях банковской системы // Решетневские чтения. 2017. Т. 2. № 21. С. 415—417.

18. *Сачков Д. И., Смирнова И. Г., Быкова В. Н.* Оценка уровня защищенности персональных данных в организациях. — Иркутск: Изд-во БГУЭП, 2015. С. 86—111.

19. *Щекочихин О. В., Шведенко В. В., Шведенко П. В.* Формальное описание информационной системы для обеспечения многоконтурного управления предприятием // Междунар. науч.-исслед. журнал. 2017. № 12—5 (66). С. 188—192.

20. *Абденов А. Ж., Заркумова-Райхель Р. Н.* Оценивание риска в информационных системах на основе объективных и экспертных оценок // Вопросы защиты информации. 2015. № 1 (108). С. 64—70.

21. *Aminzade M.* Risk assessment: The first step in improving cyber security [Электронный ресурс]. Режим доступа: https://www.helpnetsecurity.com/2017/11/13/risk-assessment/ (дата обращения: 15.01.2018).

22. *Касаткина Т. И., Гречишников Е. В., Лавлинский В. В., Здольник В. В.* Обоснование модели оценки защищенности объектов информационных технологий // Вестник Воронежского института ФСИН России. 2017. № 3. С. 65—80.

23. *Андриянова Т. А., Саломатин С. Б.* Комплексная оценка защищенности ведомственных информационных сетей // Доклады БГУИР. 2017. № 7. С. 40—44.

24. Five steps to cybersecurity risk assessment [Электронный ресурс]. Режим доступа: https://www.helpnetsecurity.com/2010/06/28/five-steps-to-cybersecurity-risk-assessment/ (дата обращения: 13.01.2018).

25. *Савченко С. О., Капчук Н. В.* Алгоритм оценки защищенности системы информационной безопасности с использованием теории игр // Россия молодая: передовые технологии — в промышленность! 2017. № 2. С. 22—27.

26. *Almasizadeh J., Azgomi M. A.* Mean privacy: A metric for security of computer systems // Computer Communications. 2014. V. 52. P. 47—59.

27. *Nazareth D. L., Choi J.* A system dynamics model for information security management // Information & Management. 2015. № 52. P. 123—134.

28. *Ажмухамедов И. М., Романов Ф. В., Князева О. М.* Определение уровня информационной безопасности на объекте информатизации на основе оценки состояния мер защиты // Вопросы защиты информации. 2015. № 3 (110). С. 66—72.

29. *Лившиц И. И.* Методика формирования численных метрик ИБ (Обзор) // Вопросы защиты информации. 2016. № 3 (114). С. 54—64.

30. *Трапезников Е. В., Данилова О. Т.* Анализ решений для оценки защищенности информации в информационных системах // Россия молодая: передовые технологии — в промышленность! 2017. № 2. С. 30—34.

31. *Трапезников Е. В.* Оценка качества системы защиты информации с помощью интеллектуальных средств: мат. Междунар. научн.-техн. конф. "Метрология, стандартизация, качество: теория и практика", 2017. С. 328—333.

32. *Трапезников Е. В.* Реализация модели анализа защиты информации на основе нейронной сети // Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 105—110.

33. *Трапезников Е. В.* Реализация системы оценки уровня защищенности информации в информационной системе. Метрология, стандартизация, качество: теория и практика. – Омск: Омский гос. техн. ун-т, 2017. С. 334—339.

34. *Трапезников Е. В., Магазев А. А.* Оценка уровня защищенности автоматизированной системы на основе марковской модели киберугроз // Южно-Сибирский научный вестник. 2019. № 3 (27). С. 95—99.

Analysis of existing methods for assessing the security of information systems

V. I. Petrenko, A. V. Sherstobitov
Federal State Autonomous Educational Institution for Higher Education
"North-Caucasus Federal University", Stavropol, Russia

The article provides a comparative analysis of methods for assessing the security of information systems. The weak and strong points of the most well-known approaches to evaluation are considered. Using the findings of this study will allow further work to improve the most optimal method for assessing the security of information systems.

Keywords: information system, security, assessment methods, information security.

Bibliography — 34 references. *Received Match 24, 2020*

УДК 004

Оптимизация операции свертки для применения в сверточных нейронных сетях при реализации в базисе ПЛИС

[1, 2] *А. С. Кущенко*; [1] *О. Б. Макаревич*, д-р техн. наук; [1] *И. Ю. Половко*, канд. техн. наук
[1] Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Таганрог, Ростовская обл., Россия
[2] АО «Научно-конструкторское бюро вычислительных систем», Таганрог, Ростовская обл., Россия

Рассмотрен классический вариант реализации сверточных фильтров, которые являются частью алгоритмов машинного обучения. Приведены преимущества программируемых логических интегральных схем (ПЛИС) перед GPU в задаче обработки изображений сверточными нейронными сетями. Предложен метод замены операции умножения на побитовую операцию xor для уменьшения необходимых ресурсов на кристалле для расчета нейронной сети. Операция умножения и побитовая операция xor неэквивалентны, но с использованием расстояния Хемминга доказана похожесть изображений. Показано, что заменять операцию умножения в сверточном фильтре можно и нейронная сеть при этом все еще будет способна выделять ключевые признаки на изображении, которые необходимы для работы сети. Проведены теоретические расчеты возможного количества вычислительных элементов после замены операции умножения на побитовую операцию xor на примере микросхемы ПЛИС Stratix 10 ф. Intel.

Ключевые слова: сверточные нейронные сети, ПЛИС, обработка изображений, искусственный интеллект.

Сверточные нейронные сети (СНС) получают все большее распространение. СНС имеют широкий круг применения: от распознавания образов на изображениях до принятия решения о направлении движения транспортных средств и поиска уязвимостей в текстах программного обеспечения [1].

Одной из главных проблем СНС является их высокая вычислительная сложность. Для вычисления СНС в реальном времени используют графические ускорители и программируемые логические интегральные схемы (ПЛИС). На этапе обучения проблема скорости вычислений стоит не так остро, так как для обучения допустимо использование высокопроизводительных систем. В реальной работе зачастую присутствуют жесткие временные рамки для вычисления СНС, а также ограничения по потребляемой мощности. При вычислении на графическом процессоре доступно несколько тысяч элементарных блоков вычислений, которые работают на частоте более 1 ГГц. Задача разработчика состоит в том, чтобы максимально эффективно формировать данные и по максимуму загружать вычислители. На графических процессорах последних поколений можно добиться времени обработки нейросетью кадра видеоизображения за 30—60 мс. Однако использование графического ускорителя не всегда оправдано. Во-первых, GPU потребляют значительное количество энергии (до 300 Вт), во-вторых, они имеют большой размер и требуют мощной системы охлаждения. Микросхемы ПЛИС последних поколений позволяют добиться сравнимых результатов по производительности, но их потребление питания меньше (до 20 Вт), они не требуют мощной системы охлаждения и могут быть размещены на одной печатной плате с управляющим процессором. Таким образом, применение ПЛИС в вычислениях нейронных сетей — достаточно перспективное направление. Однако для достижения сравнимой с GPU производительности необходимы дорогие микросхемы программируемой логики. Для обеспечения возможности вычисления на ПЛИС среднего и низкого ценового сегмента необходимо произвести оптимизацию вычисления операции свертки (наиболее ресурсоемкая операция в СНС). В данной работе рассмотрена оптимизация операции свертки двумерного сигнала (изображения).

Кущенко Андрей Сергеевич, аспирант, конструктор 2-й категории.
E-mail: andrew.kushchenko@gmail.com
Макаревич Олег Борисович, профессор, заведующий кафедрой "Безопасность информационных технологий".
E-mail: mak@tsure.ru
Половко Иван Юрьевич, доцент.
E-mail: i.y.polovko@gmail.com

Статья поступила в редакцию 9 декабря 2019 г.

Классическая свертка изображения

Классическую свертку изображения производят по формуле

$$p'_{i,j} = \sum_{k=0}^{n}\sum_{l=0}^{m} p_{i+\left(k-\frac{n}{2}\right), j+\left(l-\frac{m}{2}\right)} \times c_{k,l}, \qquad (1)$$

где i, j — индексы текущего обрабатываемого пикселя;
p — пиксель исходного изображения;
p' — пиксель результирующего изображения;
c — элемент ядра свертки;
k, l — индексы текущего обрабатываемого элемента в рамках ядра свертки;
n, m — размеры ядра свертки.

Таким образом, для вычисления одного пикселя изображения необходимо выполнить $n \times m$ операций умножения и $n \times m - 1$ операций сложения. При больших размерах ядра свертки или большом разрешении входного изображения вычисление может занимать продолжительное время.

Для оценки качества выполнения оптимизированной операции свертки был использован язык Python 3. В качестве исходного изображения было взято изображение размером 512×512 пикселей в формате RGB с глубиной цветности 8 бит на пиксель (рис. 1).

Рис. 1. Тестовое изображение

Для теста использовано ядро свертки размером 21×21. Подобный размер дает большее время вычисления, что уменьшает влияние посторонних процессов на время вычисления. Все три цветовые компоненты обрабатывали независимо друг от друга.

Время обработки изображения сверточным фильтром с указанными параметрами составило 164,753 с.

Предлагаемый вариант алгоритма свертки изображения

Для упрощения алгоритма свертки предложено реализовывать свертку изображения по формуле

$$p'_{i,j} = \sum_{k=0}^{n}\sum_{l=0}^{m} p_{i+\left(k-\frac{n}{2}\right), j+\left(l-\frac{m}{2}\right)} + c_{k,l}, \qquad (2)$$

где i, j — индексы текущего обрабатываемого пикселя;
p — пиксель исходного изображения;
p' — пиксель результирующего изображения;
c — элемент ядра свертки;
k, l — индексы текущего обрабатываемого элемента в рамках ядра свертки;
n, m — размеры ядра свертки.

Различие между алгоритмами состоит в замене операции умножения пикселей исходного изображения на элементы ядра свертки на операцию сложения.

Реализация модифицированного алгоритма с параметрами, указанными ранее, дает время вычисления 159,965 с.

На рис. 2, *а* приведен результат вычисления свертки классическим методом через умножение, на рис. 2, *б* — через сложение.

а

б

Рис. 2. Результат вычисления свертки

Как видно из рис. 2, полученные результаты похожи за исключением увеличившейся яркости. Различие в яркости возникло из-за идентичного метода нормировки и одинакового ядра свертки. При переобучении СНС с учетом нового алгоритма можно добиться схожих с исходным вариантом алгоритма результатов.

Для сравнения изображений был выбран перцептивный хеш, рассчитываемый при помощи дискретного косинусного преобразования и расстояния Хемминга [2, 3]. В качестве программной оболочки для сравнения использован ресурс pHash [4].

При вычислении перцептивного хеша с использованием дискретного косинусного преобразования по умолчанию используют порог расстояния Хемминга 26. Сравниваемые изображения имеют расстояние Хемминга 2, что говорит о том, что изображения похожи.

Особенности аппаратной реализации алгоритмов свертки на ПЛИС

Алгоритм свертки подразумевает операции сложения и умножения (также еще необходимо производить нормировку полученного изображения; для этого существует множество различных методов. Для операции сложения используют логические вентили, которые составляют большую часть микросхемы ПЛИС. Для операции умножения используют DSP-блоки (Digital Signal Processing). Стоит отметить, что количество DSP-блоков значительно меньше, чем количество логических ячеек. Для примера возьмем самую новую серию микросхем ПЛИС фирмы Intel — Stratix 10. Микросхема GX 400 содержит 378000 логических ячеек (LEs) и при этом всего 648 DSP-блоков, которые могут одновременно выполнять 1296 умножений с разрядностью операндов 18 и 19 бит, в то время как для одного сложения операндов с разрядностью 18 и 19 бит необходимо 8 LEs. Таким образом, в описанной микросхеме ПЛИС можно одновременно производить 1296 умножений и 378000/8 = 47250 сложений. Замена операции умножения на операцию сложения позволяет реализовать высокопараллельную СНС для быстрой обработки кадра изображения.

Выводы

Таким образом, можно сделать предварительное заключение о том, что замена операции умножения на операцию сложения позволяет работать СНС даже на текущих параметрах без переобучения. В работе не рассмотрено поведение реальной нейросети с новым алгоритмом, и невозможно оценить, насколько сильно улучшится или ухудшится работа СНС с использованием операции сложения вместо умножения при вычислении свертки изображений. Однако проверка похожести изображений с помощью перцептивного хеша говорит о том, что подобный механизм вычисления свертки можно применять в реальных условиях.

Использование операции сложения вместо операции умножения дает минимальный прирост в скорости работы при программной и аппаратной реализации, но в аппаратной реализации на ПЛИС появляется возможность значительного увеличения параллельности при обработке изображения. При этом необязательно использовать дорогостоящие микросхемы с большим количеством DPS-блоков, реализуя свертку на логических элементах. Для расчета сверточной нейронной сети необходимо произвести более тысячи операций свертки. При реализации свертки через сумму можно реализовать обработку всех слоев нейросети или некоторой части одновременно в конвейере. Подобный подход увеличит общую производительность за счет увеличений количества одновременно выполняемых операций свертки, а также позволит уменьшить количество обращений к внешней памяти. Уменьшение количества обращений к внешней памяти позволит снизить требования к микросхеме ПЛИС на наличие контроллеров DDR-памяти, уменьшить количество банков памяти, что, в свою очередь, упростит дизайн печатной платы и стоимость устройства [5].

Литература

1. *Беляков И. А.* Применение искусственных нейронных сетей при поиске уязвимостей в исходных текстах программного обеспечения // Изв. Петербургского ун-та путей сообщения. 2011. № 1. С. 120—129.
2. *Рудаков И. В., Васютович И. М.* Исследование перцептивных хеш-функций изображений // Наука и образование: научное издание МГТУ им. Н. Э. Баумана. 2015. № 8. С. 269—280.
3. *Чичева М. А.* Эффективный алгоритм дискретного косинусного преобразования четной длины // КО. 1998. № 18. С. 147—149.
4. *Courbariaux M., Bengio Y., David J.* Low precision arithmetic for deep learning [Электронный ресурс]. Режим доступа: https://arxiv.org/abs/1412.7024.html (дата обращения: 25.09.2019).
5. Официальная документация на контроллер внешней памяти ПЛИС ф. Altera [Электронный ресурс]. Режим доступа: https://www.altera.com/content/dam/altera-www/global/en_US/pdfs/literature/hb/external-memory/emi_plan.pdf (дата обращения: 25.09.2019).

Optimization of the convolutional operations for usage of them in convolutional neural networks, which are implemented on the FPGA basis

[1, 2] *A. S. Kushchenko,* [1] *O. B. Makarevich,* [1] *I. Yu. Polovko*
[1] South Federal University, Institute of Computer Technologies and Information Security, Taganrog, Rostov region, Russia
[2] JSC "Scientific Design Bureau of Computing Systems", Taganrog, Rostov region, Russia

This article discusses a classical implementation of convolutional filters, which are a part of machine learning algorithms. The advantages of FPGAs over GPU on the objective of image processing by convolutional neural networks was given. The method was proposed for a replacement of a multiplication operation with a bitwise operation xor to reduce necessary resources on the chip for a calculation of the neural network. Replacing the operation of multiplication with the bitwise operation xor is not equivalent, nonetheless the usage of Hamming distance has proved similarity of images. Thereby is proved that it is possible to replace the multiplication operation in a convolutional filter and the neural network still will be able to highlight the key features in the image, which are necessary for the work of the network. In the article were given theoretical calculations of the possible number of computational elements after replacement of the multiplication operation with the bitwise operation xor, by using the example of a FPGA Stratix chip. Intel.

Keywords: neural network convolution, FPGA, image processing, artificial intelligence.

Bibliography — 5 references. *Received December 9, 2019*

УДК 004.056

Методики разработки правил безопасного подключения к Internet (*Обзор*)

А. С. Вилков; *С. Л. Вилков*, канд. техн. наук; *М. М. Тараскин*, д-р техн. наук
Войсковая часть № 11928, Москва, Россия

Рассмотрены вопросы функционирования глобальной сети Internet, проблемы защищенной передачи информации в глобальной сети Internet, а также процедуры разработки правил (методик) безопасного подключения к Internet.

Ключевые слова: правила безопасного подключения к Internet, методика разработки, информационно-техническая безопасность, информационно-психологическая (психофизическая) безопасность.

С развитием технологий Internet каждая организация стремится подключить к Internet свои системы и инфраструктуры. Данная работа полезна для тех, чья организация вошла в мир пользователей системы реального времени. В таком случае необходимо позаботиться о ее защите от вмешательства извне. Проблема состоит в том, что многие разработчики политики безопасности организации рассматривают правила безопасности Internet как руководство по всеобщей защите сетей организации. Часть пользователей уже знают, что предпочтительней разрабатывать несколько документов-правил, которые охватывают различные аспекты программы защиты информации. Правила безопасности Internet являются всего лишь частью этой программы [1].

Общепринятая точка зрения на разработку правил безопасности Internet заключается в том, что их довольно легко сформулировать, поскольку об Internet знает каждый. В ряде случаев это действительно так. Тем не менее поскольку технологии меняются очень быстро, а в некоторых организациях сильна тенденция сразу внедрять новые научные открытия, довольно сложно написать правила, охватывающие все нововведения. Охватить все аспекты безопасности Internet довольно сложно, но можно использовать прагматичный подход, чтобы быть уверенным, что правилами охвачены все необходимые вопросы. Так же как было сделано с политикой безопасности вообще, правила безопасности Internet можно разбить на логические группы в соответствии с различными технологиями Internet. Опишем логические группы, на которые разбивают технологии Internet, а также дадим объяснение того, каким образом технологии отражены в разрабатываемых правилах [2].

Вилков Андрей Сергеевич, старший преподаватель.
E-mail: vilkovas2016@yandex.ru
Вилков Сергей Леонидович, преподаватель.
E-mail: vilkovas2016@yandex.ru
Тараскин Михаил Михайлович, сотрудник.
E-mail: rubico@mail.ru

Статья поступила в редакцию 18 апреля 2020 г.

Подход к разработке правил безопасности при работе с Internet

Работа с Internet может основываться на различных технологиях и требовать, соответственно, различных аппаратных и программных средств. Поэтому при разработке правил безопасности целесообразно использовать пошаговый метод. Сущность метода достаточно проста: как только выявлена проблема защиты при работе с Internet, ее сразу начинают решать с помощью разработки некоторых правил защиты. Данный метод можно использовать и в дальнейшем при расширении и/или модернизации ведомственной системы. Выделим два основных направления разработки правил безопасности:

- регламентирующих создание и функционирование интерфейса с Internet;
- для пользователей при работе с различными сервисами Internet.

Правила безопасности интерфейса связи с Internet

Как отмечалось ранее, существует достаточно большое количество технологий подключения к Internet. Интерфейсные протоколы не предоставляют никакой защиты и имеют слабые механизмы контроля входных данных. Поэтому для каждой технологии необходимо разрабатывать свои специфические правила защиты интерфейса.

Разрабатываемые правила безопасности интерфейса связи с Internet должны решать противоречивую задачу [2]: они должны, во-первых, обеспечивать безопасность передачи данных через

интерфейс, и, во-вторых, безопасность не должна препятствовать нормальному доступу к Internet.

При создании правил защиты работы с Internet необходимо учитывать уже имеющуюся архитектуру внутренней сети организации. Перестройка сети по "лучшему образцу", как правило, приводит к сильному противодействию со стороны руководства. Целесообразно достигать поставленной задачи эволюционным путем, т. е. путем пошаговых изменений при очередной модернизации сети.

Правила управления входящим трафиком

Управление входящим информационным потоком от Internet осуществляют с помощью межсетевого экрана (МЭ). МЭ представляет собой устройство, которое реализует правила управления трафиком. Данные правила определяют, какая информация пропускается во внутреннюю сеть организации и какая может передаваться из нее. При разработке правил управления трафиком необходимо учитывать место размещения МЭ в сети и режим его работы.

Существует два основных типа архитектуры связи с Internet с использованием МЭ, позволяющих разделить трафик Internet и внутренний трафик сети организации. Их объединяет наличие так называемой демилитаризованной зоны (DeMilitarized Zone — DMZ). Разница заключена в способах реализации этой зоны. Однако в любом случае создают сегмент внутренней сети, который обеспечивает изоляцию внутренней сети организации от Internet и является дополнительным элементом защиты.

Общепринятая архитектура создания DMZ приведена на рис. 1.

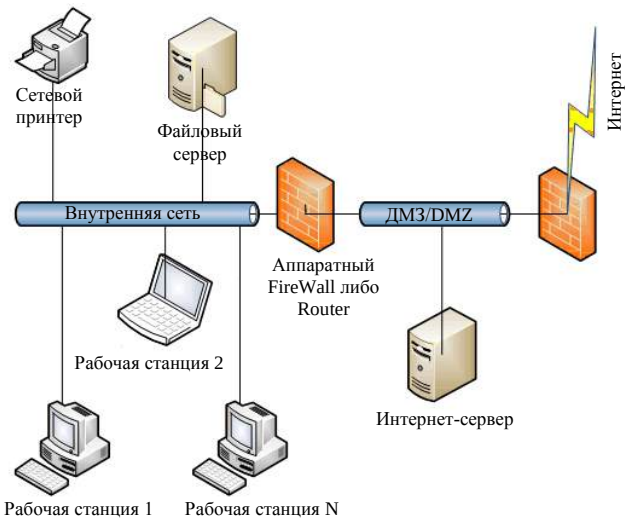


Рис. 1. Сеть с DMZ, созданная с помощью двух МЭ (N — количество ПК)

В такой архитектуре обмен данными между внутренней сетью организации и Internet всегда осуществляют только через DMZ. В самой зоне происходят проверка и фильтрация трафика по заданным правилам.

Вторая архитектура позволяет использовать один межсетевой экран. При этом DMZ создают как некий сегмент внутренней сети, который доступен пользователям (рис. 2).

Рис. 2. DMZ, который направляет трафик Internet в отдельную часть сети

Таким образом, при использовании любой архитектуры необходимо создать демилитаризованную зону, обслуживающую запросы Internet, которая защитит внутреннюю сеть организации от нежелательного трафика и при этом не будет препятствовать пользователям организации получать доступ к Internet [3].

Правила защиты интерфейса всегда привязывают к особенностям функционирования МЭ. Функции МЭ реализуют на маршрутизаторах, которые осуществляют связь с Internet. Фильтрацию трафика реализуют по определенным правилам, оформляемым как списки контроля доступа ACL (Access Control List).

Списки контроля доступа определяют набор правил, обеспечивающих дополнительный контроль над пакетами, которые принимают интерфейсы, транзитными пакетами, которые передают через маршрутизатор, а также пакетами, которые отправляют из интерфейсов маршрутизатора.

В качестве параметров для фильтрации могут быть применены проверки:

- только IP-адреса источника;
- не только IP-адреса источника, но и IP-адреса назначения;
- вложений в IP-пакеты (порты ввода-вывода приложений).

Промежуточные МЭ могут быть реализованы как на внутренних маршрутизаторах организации, так и в виде отдельных аппаратных средств. Во втором случае они не только используются для

фильтрации трафика, но и реализуют дополнительные функции [3]:

- просмотр передаваемых данных;
- кэширование часто используемых данных, что позволяет сократить трафик обмена с Internet;
- проверку сохраняемых адресов (stateful packet Inspection), что используют как часть алгоритма фильтрации пакетов для предотвращения ущерба сети искаженными пакетами;
- преобразование сетевых адресов (Network Address Translation — NAT) для сокрытия внутренней структуры сети организации от внешних пользователей (когда узлам внутренней сети необходим доступ к Internet, перед передачей внутренний IP-адрес может быть преобразован в открытый, зарегистрированный IP-адрес).

Целесообразно не привязывать разрабатываемые правила к определенным аппаратным средствам, лучше разработать правила, в которых обозначены вспомогательные процедуры, разрешенные МЭ. Это не ограничивает организацию в выборе решений при разработке правил безопасности [1].

Существует два способа составления правил, определяющих доступные вспомогательные процедуры.

В первом способе вспомогательные процедуры определяют как часть процедур администратора сети, которые предназначены для управления МЭ. Это дает возможность определять вспомогательные процедуры, поддерживающие процесс работы с Internet. При необходимости это позволяет организации добавлять новые вспомогательные процедуры, не внося изменений в документ правил. Вспомогательные процедуры, поддерживаемые шлюзом Internet, должны быть назначены комиссией, ответственной за их использование на шлюзе, и отвечать требованиям технологии [1].

Другой способ определения перечня вспомогательных процедур заключается в регламентации их в документе правил. Многие организации предпочитают определять вспомогательные процедуры в правилах, чтобы придать им больший вес. Разработка таких правил должна четко определять, на какой трафик (входящий или исходящий) они воздействуют, и учитывать используемый протокол связи с Internet [1].

Например, существует протокол пользовательских дейтаграмм (User Datagram Protocol — UDP), который не требует установления соединения. Поэтому UDP достаточно сложно управлять и контролировать. Во многих организациях появляется необходимость ограничить доступ к процедурам протокола пользовательских дейтаграмм UDP. Однако если сервер DNS, обслуживающий службы именования доменов, размещен после МЭ, то требуется сформулировать правила так, чтобы разрешить доступ пользователям Internet к порту 53 UDP. Это необходимо для распознавания адресов имен доменов организации. Следовательно, правило можно сформулировать следующим образом [1].

Шлюз Internet должен предотвращать пропуск UDP-пакетов из Internet во внутреннюю сеть организации за исключением UDP-пакетов, запрашивающих службы DNS, доступные через порт 53 [1].

Данное правило предназначено для входящего трафика, поскольку в нем сказано "из Internet в сеть организации", и не накладывает ограничений на исходящий трафик.

Работа организации с клиентами зависит от таких служб, как сетевая файловая система (Network File System — NFS), протокол передачи файлов (Network File System — FTP) и других служб, связанных с сетевыми именами. При такой формулировке правила ответы на запросы пользователей организации к "внешним" UDP-системам будут заблокированы. Следовательно, придется откорректировать правила, чтобы обеспечить работу этих служб [1].

Другая проблема возникает при работе протокола управления служебными сообщениями в сети Internet (Internet Control Message Protocol — ICMP), который передает сообщения об ошибках между компонентами сети на сетевом уровне управления. Можно заменить работу ICMP с помощью программ типа ping и traceroute (или tracert). Но данные сообщения несут информацию только о том, работает ли отдельная компонента и доступна ли она из сети [1].

При блокировании ICMP на брандмауэре теряется возможность получения ICMP-сообщений host unreachable (недоступный хост) и need to frag (необходимо разбиение). Для управления исходящим трафиком организации необходимо иметь возможность получать эти сообщения. Ввиду сложности таких решений рекомендуют не включать эти вопросы в документы, определяющие политику. Однако при желании упомянуть об этом можно составить следующую формулировку [1].

Правила для служб, базирующихся на использовании ICMP, должны определять, каким образом можно манипулировать процедурами ICMP для создания злоумышленного трафика, который может пройти незаметно. При этом должны быть учтены типы механизмов ICMP, необходимые для управления трафиком между Internet и сетью организации [1].

При формировании политики безопасности нецелесообразно обсуждать специфические правила

для служб специального назначения. Включение этих деталей в документы политики не позволит быстро вносить в систему изменения, необходимые для поддержания соответствующей среды. В большинстве случаев процедуры можно обновить за несколько минут, но изменение и экспертиза правил безопасности потребуют длительного времени [2].

Единственное исключение можно сделать для сетевых конференций, которые предназначены для распределения информации по принципу "один для всех". Основой всех этих конференций послужил сервис Usenet, используемый для общения и публикации файлов. Usenet состоит из новостных групп, в которые пользователи могут посылать сообщения. Сообщения хранятся на серверах, которые обмениваются ими друг с другом. Существует множество производственных сетевых конференций на основе данного сервиса, которые предоставляют полезную информацию. Это ведет к множеству проблем:

- опасность заражения вирусами внутренней сети при приеме файлов информации, так как механизмы антивирусной защиты отсутствуют;
- объемный трафик, не всегда соответствующий запросу пользователя.

Полный запрет использования Usenet может лишить организацию доступа к некоторым очень полезным ресурсам.

Если разрешить доступ пользователям к Usenet, то необходимо прежде всего оценить эту возможность. Организация может содержать собственный сервер или иметь доступ к серверам провайдера услуг и при этом использовать внешний сервис так, чтобы трафик Usenet не влиял на сеть организации.

В любом случае в правилах должно быть отражено, что приемлемо для использования в сетевых конференциях Usenet [1]. Можно:

- разрешить полный доступ к новостям Usenet только ограниченному кругу пользователей. Предписания политики позволят вносить в любое время поправки в список пользователей, которым предоставляют эти услуги [2];
- реализовать ограниченный доступ к сетевым конференциям Usenet. Эта поддержка распространяется на подсписок конференций, которые могут быть использованы для обеспечения деловой деятельности организации. Список конференций, к которым пользователи могут иметь доступ, регламентируется администраторами сети и может быть изменен только по письменному заявлению. В заявлении должна быть указана причина, по которой требуется разрешить доступ к конкретным конференциям. Заявления не будут удовлетворены, если не будет аргументирована производственная необходимость доступа к конференциям. Наблюдательная комиссия должна периодически проверять этот список [2].

Пользователи, допущенные к конференциям Usenet, должны пройти предварительный инструктаж и записать, в чем состоит польза от их участия в конференциях Usenet. В инструктаж обязательно входит описание того, каким образом организация предоставляет доступ пользователям к сетевым конференциям, и правила работы с Usenet. Пользователей инструктируют об использовании запатентованной в организации информации и интеллектуальной собственности [2].

Административные обязанности

После того как разработаны правила подсоединения к Internet, самое время сконцентрироваться на специфических областях, которые влияют на использование этого подключения. Начнем с правил администрирования. За исключением самых простых правил о правилах администрирования забывают, поскольку разработчики правил полагают, что все эти вопросы рассмотрены в других областях. Это может быть и так, но все же имеет смысл их описать [4].

Профилактическое обслуживание. Первая обязанность, о которой нужно знать, — это профилактическое обслуживание. В правилах должно быть требование к системным администраторам проводить регулярное обслуживание для поддержания порядка в общедоступных данных, но есть организации, которые не проводят обслуживание Web-серверов, ftp-архивов и других требующих обслуживания систем. Не выдвигая такого жесткого требования, в некоторых организациях просто игнорируют общедоступные в информационном плане части системы. Если сервер никогда не проверяют, может возникнуть ситуация, при которой Web-сервер будет взломан для того, чтобы на нем можно было хранить файлы [1].

Эти проблемы касаются не только организаций, имеющих собственные серверы. Организации, получающие услуги Internet со стороны, должны иметь правила с требованиями о том, чтобы в договоры на услуги были включены соглашения об обслуживании или профилактических работах, которые позволят администраторам организации проводить такой тип обслуживания. В любом случае следует записать в правилах, что обслуживание необходимо проводить, но в них не должно быть указано, как это будет происходить. Это относится к процедурам, а не к правилам [1].

Соглашения с внешними источниками. Соглашения с внешними источниками представляют собой довольно интересную проблему, поскольку организации вообще могут не управлять серверами. Это также становится проблемой для организаций, которые могут поддерживать собственные серверы, но управление отдельными их функциями передать внешним источникам. В таком случае достаточно иметь инструкции, но в правила следует включить требование того, чтобы обслуживание входило в условия контракта. Некоторые организации используют формулировку правил, подобную следующей [4].

Администраторы несут ответственность за процедуры обслуживания серверов, предоставляющих информацию или услуги пользователям Internet. Совместно используемые или принадлежащие внешним провайдерам серверы также необходимо обслуживать по инструкциям, согласованным в контрактах на предоставление услуг [4].

Внедрение. Администраторы также могут нести ответственность за внедрение. Даже в тех организациях, которые содержат собственный штат, ответственный за безопасность, администраторы находятся на передовой линии обороны. Они знают все о системах, сетях, а также им известны нормативы и те недостатки в сети, на которые нужно обратить внимание. Даже в более мелких организациях, где администраторы выполняют всю работу, они все равно находятся на передней линии внедрения. Несмотря на то что в других правилах должны быть полностью определены роли по внедрению, имеет смысл составить правило с формулировкой требований по внедрению подобно следующей [4].

Администраторы должны внедрять правила в соответствии с утвержденными инструкциями. Инструкции администрирования должны регламентировать контроль информации, а также защиту информации путем применения соответствующих санкций. Помимо всего прочего в эти инструкции необходимо включить требования по сохранению фактов нарушения служащими дисциплины, а также требование по применению юридических санкций в отношении внешних нарушителей правил безопасности [4].

Правила работы в WWW

Здесь речь идет о сфере деятельности настолько знакомой, что это приводит к упущениям в правилах. О Web знают все. Каждый использует Web и имеет свой собственный взгляд на соответствующие правила работы. Web может быть мощным помощником, а также источником проблем. Целью разработки правил работы в Web является обеспечение информационной безопасности организации во время такой работы без перегружения правил ненужными для пользователей и невыполнимыми запретами и ограничениями [4].

Доступ из Web к сети и инфраструктуре. Основная цель службы информационной безопасности — следить за тем, как организация обслуживает свои Web-серверы и системы, которые обеспечивают работу в Web. Постоянно появляются новые критерии безопасности, новые уязвимые места и хакерские средства. Web-узлы повреждают, похищают информацию, организация рискует из-за этих инцидентов получить негативное паблисити [4].

Помимо искажения информации существуют проблемы, связанные с воровством информации наподобие тех, которые возникают с содержимым кредитной карточки. Это говорит о том, что существуют слабые места в обслуживании таких записей или в доступе к инфраструктуре, где хранятся эти записи. Тот, чьи узлы были взломаны, знаком с данными проблемами [4].

Существует столько же способов защиты данных и сетевой инфраструктуры организации, сколько вариантов реализации Web. В ракурсе разработки правил довольно сложно предложить формулировку, удовлетворяющую конкретной системе. Однако если не обращать внимания на особенности реализации, то можно найти что-то общее во всех реализациях и изложить это в правилах [4].

Например, один из способов защиты данных заключается в установке серверов после внутреннего МЭ и применении специальных методов обеспечения более качественной связи между системами. Несмотря на то что детали такой схемы должны быть изложены в инструкциях, в качестве руководства для тех, кто внедряет эту систему, нужно разработать правило. Формулировка правила может быть следующей [4].

Все системы с собственными и клиентскими данными, которые поддерживают Web-сервер, нельзя устанавливать на том же сегменте сети, на котором установлены Web-серверы. Эти вспомогательные серверы необходимо устанавливать таким образом, чтобы доступ был возможен только к Web-серверам. Организации следует установить надлежащие средства контроля для обеспечения гарантий того, что вспомогательные серверы могут быть доступны только способом, согласованным с функциями, на которые они запрограммированы [4].

Другая проблема заключается в выполнении программ, сценариев или иных вспомогательных процедур на Web-сервере. Некоторые организации не испытывают таких проблем и разрешают запускать сценарии, которые работают как часть общего шлюзового интерфейса сервера (Common Gateway Interface — CGI). В других организациях испытывают беспокойство при разрешении запуска всего, что отличается от тестовых страничек сервера. Необходимо быть очень осторожным при утверждении таких правил, поскольку они будут сильно влиять на архитектуру вспомогательных систем Internet организации. Чрезмерная жесткость правил будет неприемлема для организаций, которые пользуются услугами внешних вспомогательных систем [4].

На Web-серверах должны запускаться только проверенные программы и сценарии, которые функционируют как часть общего со вспомогательными Web-системами шлюзового интерфейса (CGI). Все другие программы необходимо выполнять на иных системах, не связанных с Web-системами, на которых эти сценарии работают как посредники для такого выполнения [4].

Защита и обслуживание CGI и других сервисных программ

Поразмышляем о производительности Web-сервера при пересылке динамической информации через различные интерфейсы. Эти интерфейсы запрограммированы с использованием сценариев, встроенных команд или языков программирования, которые создают определенные проблемы при защите серверов. Наибольшая опасность заключается в том, что в таких программах могут возникать случайные ошибки, алгоритмические ошибки или другие проблемы, связанные с языком программирования. Языки сценариев имеют команды, выполняемые внешними программами, в которых могут быть свои ошибки, бреши в защите или незадокументированные особенности, тоже способные привести к нарушениям безопасности [5].

Когда цикл разработки системы происходит в "эпоху Internet", возникает множество неожиданных проблем в программах в связи с тем, что их эксплуатируют пользователи, а поставляют разработчики. Не вдаваясь в тонкости развития программного обеспечения, укажем, что правила должны учитывать практику с требованиями присутствия программного обеспечения "вчерашнего дня". Эти правила также не должны быть связаны с правилами разработки программного обеспечения [5].

При разработке правил для этих вспомогательных программ необходимо рассмотреть два аспекта:

- ревизию всего установленного программного обеспечения на предмет возникновения любых потенциальных проблем;
- безопасную эксплуатацию этих средств.

Ревизия программ на предмет выявления ошибок и брешей в защите обычно представляет собой важный этап процесса разработки программного обеспечения, но существует тенденция сдавать в эксплуатацию программное обеспечение, не проведя надлежащего тестирования. Разработав правило, требующее провести такую ревизию, можно надеяться, что разработчики потратят немного дополнительного времени на обеспечение гарантий того, что с этими программами не будет проблем. Формулировка правил может выглядеть следующим образом [5].

Вспомогательные программы для Web-серверов требуется обязательно подвергать тщательной проверке всех компонентов. Во время ревизии проверяют рабочие характеристики этих программ на предмет непредвиденных результатов по причине сбоев в работе. Кроме того, в процессе ревизии необходимо рассмотреть возникшие проблемы безопасности системы и сети [5].

Сосредоточимся непосредственно на элементах программного обеспечения. Существуют два аспекта, по поводу которых стоит беспокоиться. Во-первых, если какой-либо элемент программного обеспечения не используют, его не надо загружать или надо выбрать такую конфигурацию, чтобы сервер его не использовал. Другая проблема состоит в том, что когда эти элементы используют, следует позаботиться о проблемах безопасности, выявленных исследовательскими группами безопасности, поставщиками и взломщиками. Иногда создается впечатление, что предостережения касательно брешей в защите серверов или программ, генерирующих содержимое, возникают еженедельно [5].

Правила в этих областях довольно сложно трактовать. Если организация использует внешние Web-серверы, то определить их потенциальные проблемы довольно сложно. Можно попробовать заключить соглашение при подписании контракта, согласованное с правилами организации, но все равно это будет намного сложнее, чем при наличии у организации собственных Web-серверов. Администраторы не могут просто проводить новые патчи (заплатки) или менять конфигурацию, так как не могут быть уверены в том, что эти обновления не приведут к неправильной работе или к выходу из строя сервера или программного обеспечения [5].

Существует слишком много вариантов решения данных проблем, поэтому их невозможно решить, составив всего лишь одну формулировку правил. В следующем примере из нескольких различных правил извлечены общие положения и составлена одна общая формулировка. Организации предлагается использовать следующий пример в качестве руководства по разработке собственного правила, а не в качестве образца, который можно вставить в правила.

Web-серверы должны быть установлены и сконфигурированы так, чтобы обеспечить функционирование только тех вспомогательных систем, которые необходимы для поддержки операционной среды. Администраторы должны отслеживать сообщения систем оповещения о нарушениях безопасности на предмет обнаружения уязвимых мест в установленных компонентах системы. Для тестирования и проведения патчей в установленных компонентах системы администраторы должны работать совместно с программистами и ответственными за информацию лицами [6].

Корректировщики содержимого

Корректировщики содержимого представляют собой языки программирования и языки подготовки сценариев, называемые run anywhere enhancers. Сценарии и апплеты загружают с сервера для корректировки содержимого при интерактивном взаимодействии с пользователем. Проблема заключается в том, что в браузерах, обеспечивающих соответствующий сервис, найдены уязвимые места в защите. В результате некоторые организации вынуждены отказаться от использования серверов Internet.

Можно найти технические решения, чтобы программы корректировки содержимого не включать в сеть. К сожалению, пользователи могут и не иметь возможности пользоваться узлами, которые оснащены этими корректировщиками. Несмотря на развитие технологии и уменьшение количества проблем с защитой, организация должна рассмотреть общее влияние на безопасность при включении таких корректировщиков в сеть.

Управление содержимым

Концепция состоит в том, что одно лицо или ведомство назначают ответственным за информацию, относящуюся к определенному бизнес-процессу. Таким образом, создают систему защиты данных и устанавливают ответственность за ее целостность и безопасность. В отношении Web-серверов все должно быть точно так же. Даже в том случае, если организация заключает договор о Web-услугах, кто-то из организации должен отвечать за содержимое [3].

В каждой Web-системе есть несколько способов управлять содержимым. Поэтому довольно сложно составить правила, в которых в достаточной мере будут учтены все способы управления данными. Проблема заключается в том, что правила должны определять не только ответственных за содержимое, но также и то, каким образом это содержимое изменять и управлять им [3].

Правило конфиденциальности

Наиболее спорный аспект, касающийся Web-серверов, заключается в том, как распоряжаются информацией ответственные за нее лица после ее получения из соответствующих вспомогательных систем. Эксперты в области безопасности обеспокоены тем, что при поисках нужного содержимого и достижении удобства пользования бывает выдано слишком много личной информации. Создается впечатление, что каждый беспокоится о конфиденциальности и занимается поиском собственников Web-серверов, чтобы продемонстрировать свое добропорядочное гражданство, а также раскрыть, каким образом он использует собираемую информацию. Это раскрытие определяет правило конфиденциальности [3].

Следование правилу конфиденциальности несколько отлично от следования правилу раскрытия информации. Правило конфиденциальности представляет собой общедоступную формулировку и разъясняет пользователям, какую личную информацию можно собирать и как организация планирует распорядиться этими данными. По причине непостоянства правила конфиденциальности не рекомендуется включать его в документы правил информационной безопасности. Однако необходима рекомендация, как создать документ, доступный каждому для прочтения. Формулировка правила может выглядеть следующим образом [3].

На Web-серверах должно находиться общедоступное правило конфиденциальности, разъясняющее, какую информацию можно собирать и что организация может делать с этими данными. Правило конфиденциальности должно быть общедоступным на основе подключения к обслуживаемым страницам [3].

Доступ пользователей к Web. Главное при создании правил доступа пользователей заключается в том, что пользователям доверять нельзя. Других

правил, собственно, и не существует. При отсутствии правил и ограничивающих инструкций организации столкнутся с большими сложностями, поскольку пользователи будут посещать любой сайт, загружать любые программы, будут иметь доступ к аплетам и заполнять любую форму, какую пожелают [3].

Во многих организациях принято работать по правилам, которые включают фильтрацию содержимого. Фильтры содержимого обычно не допускают посещения пользователями сайтов, которые компания считает незаконными или в каком-то смысле аморальными. Кроме того, они предоставляют кэши содержимого на шлюзах Internet, чтобы ускорить загрузку информации. Другие возможные фильтры содержимого могут не допускать использование аплетов корректировки содержимого [3].

Независимо от сферы деятельности организации правила должны четко разъяснять, каким образом управлять трафиком в Internet. Пользователям необходимо давать разъяснения скорее с точки зрения законности действий, чем с какой-то другой. Нужно отметить, что организация контролирует трафик и может даже проводить аудит, чтобы определить, какую информацию передают через интерфейс Internet. Если не сообщить об этом, а также не предупредить о дисциплинарных взысканиях, утвержденных правилами, то организация может оказаться втянутой в судебные процессы, инициированные служащими. Приведем примерную формулировку правил [3].

Пользователи, имеющие доступ к Internet, не должны посещать сайты, которые созданы с нарушениями закона или содержат оскорбительную информацию о пользователях. Организация должна сохранить за собой право блокирования доступа ко всем сайтам, считаемым неприемлемыми, а также делать регистрационные записи о посещении сайтов всеми пользователями, на основании которых в любое время можно провести аудиторскую проверку. В качестве этапа процесса фильтрации содержимого организации должно быть разрешено установить систему кэширования [3].

Представители одной организации-провайдера выразили беспокойство по поводу, не будут ли правила ограничивать их пользователей в создании Web-страниц. Они утверждали, что это является расширением их творческой активности, и по этой причине не хотели останавливать такую практику. Провайдеры уверяли, что никто не будет злоупотреблять своими привилегиями [3].

Однако, во время исследования сети организации извне с помощью некоторых стандартных средств удалось обнаружить все серверы, обслуживающие Web-системы. В результате тестирования были обнаружены серверы на нестандартных портах. На основании этой информации были преобразованы адреса поиска, чтобы установить, какому имени какой адрес соответствует. Обнаружилось, что один из адресов имеет резервное имя, зарегистрированное в InterNIC (Internet Network Information Center — информационный центр сети Internet). Используя новое имя, эксперт получил доступ к сайту. То, что удалось обнаружить на этом сайте, шокировало людей, с которыми он сотрудничал. Информация совершенно не соответствовала целям организации и могла считаться запрещенной [6].

Поскольку все это происходило только на этапе разработки правил, не было никакой возможности наложить дисциплинарное взыскание на конкретного служащего. Конечно, можно было применить некоторые санкции, но не столь серьезные, как хотелось бы. Это подтолкнуло к разработке правила, которое выглядит так [6].

Служащим организации нужно разрешить создавать неофициальные сайты в сети организации. Эти Web-сайты должны быть доступны только внутри организации. Пользователи, которые хотят, чтобы содержимое их сайтов было доступно из Internet, должны, прежде чем сделать свои страницы доступными, предоставить их для просмотра комиссии, возглавляемой арт-директором. Арт-директор должен использовать правила в качестве руководства, по которому производят ревизию сайта. Он также отвечает за решения об отказе в праве доступа к сайту или его разрешении [6].

Это правило было сформулировано для организации, в которой насчитывалось меньше 75 пользователей, чьи Web-серверы были размещены у ближайшего провайдера услуг. Внедрение данного правила в дальнейшем избавило организацию от проблем с генерируемым пользователями содержимым [6].

Ответственность за приложения

По большей части ответственные за данные и процессы лица не столь осведомлены в тонкостях технологии, как программисты или администраторы. Даже те, кто начал свою карьеру как "технарь", сейчас обнаруживают себя во власти приложений, которые развертывают и с которыми работают в системе информационной безопасности организации.

Правила работы в Internet, касающиеся приложений, должны касаться только защиты данных и пересылки файлов, а также аутентификации во

время этих пересылок. Прочие аспекты безопасности приложений следует включить в правила, относящиеся к другим сферам деятельности, таким как разработка программного обеспечения организации собственными силами. Если не усложнять эти вопросы, можно сфокусировать внимание в пределах сферы интересов организации.

Пересылка данных и файлов

Каждый протокол обеспечивает определенный способ пересылки данных между пользователями с различной степенью защищенности. Несмотря на то что все протоколы служат всего лишь для пересылки данных, некоторые из них не гарантируют, что данные дойдут по назначению. Их используют для того, чтобы быть уверенными в достоверности пересылаемых данных. На самом деле это вовсе не так. Надежное завершение передачи данных и файлов зависит от протоколов верхних уровней, взаимодействия программ, а также вмешательства людей.

Ситуация с безопасностью усложняется еще и существованием вероятности того, что человек или программа могут перехватить пересылаемую в Internet информацию и прочитать ее. Данные организации могут быть считаны любым, кто имеет доступ к инфраструктуре Internet во время передачи. Обычно его называют человеком в центре атаки.

Прочитав последние два абзаца, можно задаться вопросом: где здесь говорится о правилах безопасности? Суть заключается не в создании правил, регламентирующих защиту. Правила должны рекомендовать ответственным за информацию пользователям возможность осознать, какую роль играют приложения при пересылке файлов, а также обеспечить защиту этих данных. Это довольно просто сделать, написав формулировку правил, подобную следующей.

Ответственные за информацию и процессы лица должны оценивать все приложения с точки зрения того, обеспечена ли безопасность пересылки данных и файлов в соответствии с требованиями, выдвигаемыми бизнесом. Помимо всего прочего в защиту пересылаемых данных необходимо включить обеспечение гарантий того, что данные доходят по назначению и не могут никем быть считаны в процессе пересылки.

Эта формулировка правил написана в самом обобщенном виде и подразумевает применение для обеспечения безопасности пересылки только шифрования. Тем не менее этого вполне достаточно, чтобы лица, ответственные за развертывание приложений и за распространение данных организации, учитывали последствия от принятых ими решений.

Аутентификация транзакций Internet

С нарастанием популярности Web-технологий пользователи сталкиваются со старыми проблемами в новой форме. При предоставлении услуг посредством Web используют модель, в которой применяют так называемый обмен блоками (block mode transfer). Широко применяемый в старых вычислительных системах обмен блоками функционирует следующим образом: блок данных пакуется с экрана, передается на удаленную систему, а затем блок данных принимается взамен. Однако в среде Web соединение между сервером и клиентом прерывается после завершения передачи данных.

Аутентификация представляет собой идентификацию пользователя в системе, на сервере или в программном обеспечении, разрешающую ему использовать эти средства. Аутентификацию осуществляют многими способами, но общепринято требовать, чтобы пользователь вводил идентификационные данные и пароль. Сущность блочной передачи данных при работе в Web представляет интересные проблемы не только в отношении аутентификации транзакций, но и при создании среды, где пользователь не должен каждый раз идентифицироваться при подключении к серверу.

В правилах аутентификации должно быть записано, что ответственные за данные и процессы лица обеспечивают определение личности тех, кто обращается к данным. Речь идет не только о пользователях Internet, но и о партнерах, которые могут иметь доступ через виртуальные частные сети. В правилах также должны быть учтены все транзакции Internet, включая пересылки Web, подключения к базам данных и терминальным службам.

Типичная формулировка правил выглядит следующим образом.

Ответственные за данные и процессы лица должны гарантировать, что реквизиты всех пользователей патентованных данных проверяются и принадлежат этим пользователям. Ответственные за данные и процессы лица должны разработать процедуры подтверждения и отмены права на выполнение этих операций [3].

Модемы и прочие лазейки

Еще один способ расширить доступ к своим сетям состоит в использовании модемов. Одни орга-

низации эксплуатируют модемные накопители, управляемые отдельными серверами, которые защищают и поддерживают соединения с внешними пользователями. Другие устанавливают модемы на специальных серверах, которые предоставляют доступ минимальному количеству пользователей. Независимо от применяемого метода общим является то, что администраторы контролируют модемный доступ централизовано [1].

Профессионалы в области безопасности считают, что централизованное управление модемами является ключевым моментом в управлении устройствами, обеспечивающими временный доступ. Таким образом, они могут контролировать и управлять процессом, не прерывая предоставление услуг. Чего они не желают позволить, так это установки модемов в разных местах сети. Модем, установленный в системе пользователя, которая сконфигурирована для ответов на входящие звонки, является потенциальной точкой доступа для тех, кто хочет взломать сеть [3].

Пользователи часто подмечают, что могут установить модемы в своих системах, в которых работают программы, способные обеспечить удаленный доступ к их файлам. Эти программы представляют собой хорошо известные проблемы для информационной защиты, позволяющие любому, кто подключается к модему, получить доступ в систему и к сети, к которой эта система подключена. Более того, поскольку эти модемы не контролируют, администраторы не смогут остановить взломщика до нанесения ущерба [1].

Помимо атак на отказы в обслуживании (denial of service attacks) существует еще одна очень серьезная проблема — это модем, установленный в сети, которая неправильно сконфигурирована. Если пользователям требуется разрешение для подключения к сети, то администраторы предпочтут иметь правила, позволяющие им управлять доступом. Они потребуют внести в правила запрет на установку модемов без их разрешения. В таком случае в правила можно включить следующее предложение [1].

Пользователи не должны устанавливать модем в своих системах или в любом месте сети без соответствующих санкций.

Отметим, что эта формулировка допускает исключения, но они должны быть санкционированы. В данных правилах не уточняется, что представляют собой "соответствующие санкции". Остается руководствоваться принятыми в организации инструкциями по проведению контроля.

Не каждой организации нужен модемный доступ к сети. Одни организации могут установить всего несколько модемов и разработать правила, обеспечивающие требуемую конфигурацию и соответствие стандартам безопасности. Другие организации поддерживают большое количество модемов, позволяющих пользователям наборный доступ, соединение с сервером и аутентификацию непосредственно в сети. Независимо от требований организации правила безопасности должны поддерживать роль администраторов в контролировании и обслуживании вспомогательных систем [1].

Если в организации используют модемный накопитель, подключенный к централизованно управляемому серверу, который обеспечивает строгую аутентификацию, формулировка правил может быть следующей.

Системы коммутации должны устанавливаться и управляться системными администраторами. Пользователи, желающие получить доступ в сеть посредством модема, должны при подключении проходить аутентификацию. В эту аутентификацию необходимо включить компонент безотказности [3].

В формулировке не указано, насколько строгим должен быть подход к аутентификации. Вводя лишь "компонент безотказности", внедрение аутентификации не связывают только с одним ее типом. Это предполагает, что будет использован некий строгий алгоритм привязки процесса к определенному пользователю. Он может быть каким угодно, начиная с алгоритма PKI и заканчивая аутентификацией с использованием устройств идентификации. Гибкость заключается также в том, что когда биометрия станет доступным средством, может быть использована технология на ее основе, и не будет необходимости изменять правила [1].

Очевидно, что исходным посылом для инициирования методик разработки правил безопасного подключения к Internet должны являться данные об общем состоянии защищенности объекта. В свою очередь, эффективное оценивание состояния защищенности объекта невозможно без разработки методик анализа защищенности.

Методика анализа защищенности

Пока что не существует каких-либо стандартизированных методик анализа защищенности АС, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки можно. Хотя данная методика и не претендует на всеобщность, ее эффективность многократно проверена на практике [7].

В типовой методике включает используют следующие методы:

- изучение исходных данных по АС;
- оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- ручной анализ конфигурационных файлов маршрутизаторов, МЭ и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS серверов, а также других критических элементов сетевой инфраструктуры;
- сканирование внешних сетевых адресов ЛВС из сети Internet;
- сканирование ресурсов ЛВС изнутри;
- анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных агентов.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника по преодолению механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование можно производить вручную либо с использованием специализированных программных средств [7].

Исходные данные по обследуемой АС

В соответствии с требованиями РД ФСТЭК России при проведении работ по аттестации безопасности АС, включающих предварительное обследование и анализ защищенности объекта информатизации, заказчиком работ должны быть предоставлены следующие исходные данные [2, 5]:

- полное и точное наименование объекта информатизации и его назначение;
- характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации (в соответствии с какими перечнями определен: государственным, отраслевым, ведомственным, предприятия);
- организационная структура объекта информатизации;
- перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывают указанную информацию (расположенных в помещениях, где она циркулирует);
- особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны;
- структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией;
- общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации;
- наличие и характер взаимодействия с другими объектами информатизации;
- состав и структура системы защиты информации на аттестуемом объекте информатизации;
- перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию;
- сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ;
- наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных);
- наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывают защищаемую информацию и хранят информационные носители);
- наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Опыт показывает, что перечисленных исходных данных недостаточно для выполнения работ по анализу защищенности АС. Приведенный в РД ФСТЭК России список нуждается в расширении и

конкретизации. Последний пункт приведенного списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти "дополнительные" данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС [8].

Дополнительная документация:

- нормативно-распорядительная документация по проведению регламентных работ;
- нормативно-распорядительная документация по обеспечению политики безопасности;
- должностные инструкции для администраторов, инженеров технической поддержки, службы безопасности;
- процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам;
- схема топологии корпоративной сети с указанием IP-адресов и структурная схема;
- данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса;
- размещение информационных ресурсов в корпоративной сети;
- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- схемы размещения линий передачи данных;
- схемы и характеристики систем электропитания и заземления объектов АС;
- данные по используемым системам сетевого управления и мониторинга;
- проектная документация;
- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений.

Эксплуатационная документация:

- руководства пользователей и администраторов, используемых программных и технических средств защиты информации (СЗИ) (в случае необходимости);
- анализ конфигурации средств защиты внешнего периметра ЛВС;
- при анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

– настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;

– используемые схемы и настройка параметров аутентификации;

– настройка параметров системы регистрации событий;

– использование механизмов, обеспечивающих сокрытие топологии защищаемой сети, включающих в себя трансляцию сетевых адресов (NAT), маскарадинг и использование системы split DNS;

– настройка механизмов оповещения об атаках и реагирования;

– наличие и работоспособность средств контроля целостности;

– версии используемого ПО и наличие установленных пакетов программных коррекций.

Методы тестирования системы защиты

Тестирование системы защиты АС проводят в целях проверки эффективности используемых в ней механизмов защиты, их устойчивости в отношении возможных атак, а также поиска уязвимостей в защите [9]. Традиционно используют два основных метода тестирования:

- "черного ящика";
- "белого ящика".

Тестирование по методу "черного ящика" предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний проводят все известные типы атак и проверяют устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод "белого ящика" предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяют наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличии уязвимостей делают на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяют на практике. Основной инструмент анализа в данном случае — это программные агенты средств анализа защищенности системного уровня, рассматриваемые в [9].

Таким образом, правила безопасности Internet довольно сложно разрабатывать из-за быстрого изменения технологий. Вместо того чтобы разра-

батывать одно общее правило, разработчик может подойти к разработке правил безопасности Internet, разбив известные технологии на логические группы и создавая правило для каждой области применения [1].

Подход к Internet.

- Прежде чем разрабатывать правила для Internet, необходимо определить количество вопросов, которые должны быть отражены в этих правилах. На первом этапе необходимо разобраться в основах архитектуры, а также понять значение брандмауэра и преобразования сетевых адресов.
- Следующий шаг заключен в определении вспомогательных процедур, которые могут пропускаться через шлюз. Чтобы понять, что именно рассматривать, может оказаться полезным классифицировать вспомогательные процедуры по типу протоколов, а также по их принадлежности к входящим или исходящим процедурам.
- Затем необходимо определить различия между приложениями (промежуточными звеньями, фильтрацией пакетов и проверкой сохраняемых адресов на брандмауэре).

Административные обязанности.

- Правила, регламентирующие административные обязанности, должны предписывать обеспечение определенного уровня поддержки работы систем, являться частью правил группы обеспечения правовых санкций.

Правила работы в WWW.

- Если организация располагает собственной службой Web или пользуется внешними источниками, из которых возможен доступ к сетевой инфраструктуре организации, для защиты этого интерфейса также необходимо иметь соответствующие правила.
- Правила защиты и сопровождения сервисных программ и сценариев должны предписывать ревизию этих программ на предмет безопасности и наличия ошибок. Кроме того, необходимо рассмотреть сопровождение и обеспечение защиты средств, поставляемых извне, используемых для поддержки Web-услуг.
- В некоторых организациях хотят иметь правила управления информацией, находящейся на Web-узле. В ином случае лицам, ответственным за данные и процессы, предоставляется право определять, какой информацией они должны управлять.
- Самый спорный аспект услуг Web заключается в том, что могут делать ответственные за информацию с собранной информацией. С этим проблем быть не должно: необходимо ввести правила, делающие общедоступным правило конфиденциальности, которым следует руководствоваться при получении Web-услуг.
- При разработке правил работы в Web нельзя забывать о пользователе. В правилах должна быть короткая формулировка, в которой будет определена ответственность пользователей при использовании ими Internet.

Ответственность за приложения.

- Ответственные за приложения и процессы лица должны нести ответственность за пересылаемую информацию, а также за ее надежность и обеспечение гарантий того, что информация распространяется только среди пользователей, которым даны соответствующие полномочия.
- Правила разработки приложений могут зависеть от правил разработки программного обеспечения или всего лишь предписывать руководствоваться в этом деле передовым опытом.
- Для получения доступа к данным следует запросить приложения, которые идентифицируют внешних участников обмена через Internet, а также обеспечат расширенную аутентификацию пользователей, обращающихся к Internet. Так должны работать все приложения, получающие доступ к данным организации.

Модемы и прочие лазейки.

- Еще один способ расширить доступ к сети организации заключается в использовании модемов. Помимо атак на отказы в обслуживании серьезная проблема заключается в установке модема на неправильно сконфигурированной сети. Для руководства тем, где и как устанавливать модемы, также можно разработать правила.
- Те, кто организовал модемный доступ к сети, должен позаботиться о разработке правил, которые разрешат администраторам централизованный мониторинг и управление этими модемами.
- Поскольку получить доступ к модемам может кто угодно, полезно разработать правила, которые предписывают строгую аутентификацию тех, кто получает доступ к сети.

Приведенный обзор методик разработки правил безопасного подключения к Internet в целом охватывает различные стороны работы с ним: *информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека).* Применение на практике представленных в материалах работы методик обеспечит повышение эффективности защиты информации на различных этапах использования Internet в организациях.

Литература

1. Межсетевые экраны [Электронный ресурс]. Режим доступа: http://www.intuit.ru/studies/professional_skill_improvements/14591/courses/1286/lecture/24241.
2. Иллюстрированный самоучитель по разработке безопасности [Электронный ресурс]. Режим доступа: http://samoychiteli.ru/document34444.html.
3. Иллюстрированный самоучитель по разработке безопасности [Электронный ресурс]. Режим доступа: http://adminbook.ru/index.php?men1=7_1/6/2.
4. Политика безопасности при работе в Интернете [Электронный ресурс]. Режим доступа: http://www.safe-inform.ru/11b/glava-06-tablica-6-1-vspomogatelnye-sistemy-rassmatrivaemye.htm.
5. *Бармен С.* Разработка правил информационной безопасности. — М.: Вильямс, 2002. – 208 с. ISBN 5-8459-0323-8.
6. Иллюстрированный самоучитель по разработке безопасности [Электронный ресурс]. Режим доступа: http://computers.plib.ru/security/Development%20of%20safety/menu.html.
7. Анализ защищенности корпоративных автоматизированных систем [Электронный ресурс]. Режим доступа: http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem.
8. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/901817219.
9. Аудит безопасности ИТ-инфраструктуры предприятия: стратегия тестирования и основные моменты [Электронный ресурс]. Режим доступа: https://ipiskunov.blogspot.com/2016/07/blog-post_8.html.

Methodology for the development of rules for safe Internet connectivity (*Review*)

A. S. Vilkov, S. L. Vilkov, M. M. Taraskin
Military unit No. 11928, Moscow, Russia

The article deals with the functioning of the global Internet network, the problems of secure information transfer in the global Internet network, as well as the procedure for developing rules (techniques) for secure Internet connection.

Keywords: rules for safe Internet connection, development methodology, information and technical security and information, psychological (psychophysiological) security.

Bibliography – 9 references. *Received April 18, 2020*